LEONHARDI EULERI
OPERA OMNIA

SUB AUSPICIIS
SOCIETATIS SCIENTIARUM NATURALIUM
HELVETICAE

EDENDA CURAVERUNT

FERDINAND RUDIO
ADOLF KRAZER PAUL STÄCKEL

SERIES PRIMA
OPERA MATHEMATICA
VOLUMEN SECUNDUM



LIPSIAE ET BEROLINI
TYPIS ET IN AEDIBUS B. G. TEUBNERI
MCMXV

LEONHARDI EULERI

COMMENTATIONES ARITHMETICAE

VOLUMEN PRIMUM

EDIDIT

FERDINAND RUDIO



LIPSIAE ET BEROLINI
TYPIS ET IN AEDIBUS B. G. TEUBNERI
MCMXV

VORWORT DES HERAUSGEBERS

Nach dem Einteilungsplane der Gesamtausgabe von LEONHARD EULERS Werken werden die zahlentheoretischen Abhandlungen unter dem Titel *Commentationes arithmeticae* vier Bände füllen, nämlich die Bände 2—5 der ersten Serie. Das Redaktionskomitee war sich von Anfang an darüber klar, daß innerhalb dieser Bände keine andere Anordnung als die nach den Druckjahren gewählt werden könne, entsprechend der ersten Abteilung von G. ENESTRÖMS *Verzeichnis der Schriften LEONHARD EULERS*. Die wenigsten zahlentheoretischen Abhandlungen EULERS sind ihrem Inhalte nach derart abgegrenzt, daß ihre Einreihung in einen nach Materien geordneten Plan auf unzweideutige Weise durchführbar wäre. In dieser Überzeugung ist das Redaktionskomitee auch von einem der besten Kenner der EULERSCHEN Zahlentheorie bestärkt worden, von DEDEKIND. Es ist dem Komitee ein Bedürfnis, dem hochverehrten Herausgeber von DIRICHLETS *Vorlesungen über Zahlentheorie* den ehrerbietigsten Dank auszusprechen für das tatkräftige Interesse, das er als einer der Ersten der Euleransgabe entgegengebracht hat.

Der vorliegende erste Band der *Commentationes arithmeticae*, der mit Abhandlung 26 des ENESTRÖMSCHEN Verzeichnisses beginnt und mit Abhandlung 279 schließt, umfaßt mit 26 Abhandlungen die Druckjahre 1738—1764. EULER war 1727 nach Petersburg gekommen, ist 1741 nach Berlin übergesiedelt und 1766 nach Petersburg zurückgekehrt. Es handelt sich also in unserem Bande um den ersten Petersburger und fast den ganzen Berliner Aufenthalt. Von den 26 Abhandlungen sind aber alle bis auf drei, nämlich die Abhandlungen 100, 152 und 175, in den Denkschriften der Petersburger Akademie erschienen, und zwar 7 in den Bänden 6—14 der Commentarii (1738—1751) und 16 in den Bänden 1—9 der Novi Commentarii (1750—1764).[1] Abgesehen von der einen Abhandlung 158 *Observationes analyticae variae de combinationibus* sind alle Abhandlungen des vorliegenden

1) Es ist nicht ohne Bedeutung, darauf zu achten, daß der letzte Band der alten Commentarii ein Jahr nach dem ersten Bande der neuen herausgegeben wurde. In diesem ersten Bande der neuen Serie befindet sich die Abhandlung 134, in jenem letzten der alten die Abhandlung 164. Siehe hierzu die Anmerkung p. XX.

Bandes auch in der bekannten, verdienstvollen Sammlung enthalten, die 1849 von den Urenkeln EULERS, den Brüdern P. H. und N. FUSS, herausgegeben worden ist[1]. Diese Abhandlung 158 gehört aber ihrem Hauptinhalte nach zu dem, was bei EULER *Partitio numerorum* heißt, und steht im engsten Zusammenhange mit den beiden Abhandlungen 191 *De partitione numerorum* und 394 *De partitione numerorum in partes tam numero quam specie datas*. Da diese beiden in die Sammlung der Brüder FUSS aufgenommen worden sind, so ist nicht recht zu verstehen, warum die Abhandlung 158 damals ausgeschlossen wurde.

Bekanntlich sollten die von P. H. und N. FUSS herausgegebenen *Commentationes arithmeticae* nur den Anfang bilden zu einer Gesamtausgabe[2]) der Abhandlungen EULERS und so erschienen sie denn auch unter dem weiteren Titel *LEONHARDI EULERI Opera minora collecta*. Ebenso ist bekannt, daß das Unternehmen nicht durchgeführt werden konnte und schließlich 1862 mit der Herausgabe der *Opera postuma* sein Ende fand. Trotz diesem Mißerfolg aber muß dankbar anerkannt werden, daß die Sammlung der Brüder FUSS eine wichtige wissenschaftliche Mission erfüllt hat. Sie hat Jahrzehnte hindurch einen bequemen Zugang zu den unvergänglichen arithmetischen Schöpfungen EULERS gewährt und hat es ermöglicht, daß die Schätze, die in den alten, nicht für Jeden erreichbaren Denkschriften niedergelegt sind, Gemeingut der Mathematiker werden konnten. Es sei daher gestattet, diese wichtige Veröffentlichung noch etwas genauer zu besprechen und sie in Beziehung zu der neuen Ausgabe zu setzen.

Auch in den *Comment. arithm.*[3]) ist die chronologische Ordnung gewählt, aber nicht nach den Druckjahren, obwohl diese doch als die einzig sichere erscheint, sondern nach den Exhibitionsdaten. Das Redaktionskomitee der Euleraussgabe hat aber nicht nur die Ordnung nach den Druckjahren für geboten erachtet, und zwar innerhalb einer jeden Abteilung der ganzen Ausgabe, sondern es hat auch vorgesehen, daß jeder Abhandlung die ihr zukommende Nummer des ENESTRÖMSCHEN Verzeichnisses als bleibende Signatur, nach der auch zitiert werden soll, beigefügt werde. Und um diese Bezeichnung noch stärker und reinlicher hervortreten zu lassen und um allen Verwechselungen aus dem Wege zu gehen,

---

1) *LEONHARDI EULERI Commentationes arithmeticae collectae.* Ed. P. H. et N. FUSS, 2 t., Petropoli 1849.

2) Genaueres hierüber findet man in dem *Vorwort zur Gesamtausgabe der Werke von LEONHARD EULER, LEONHARDI EULERI Opera omnia*, series I, vol. 1, ferner in dem von P. H. FUSS verfaßten *Prooemium* der *Commentationes arithmeticae*, t. I, p. VII–XXVII, LXXXI–LXIII, und namentlich in dem Buche von P. STÄCKEL und W. AHRENS, *Der Briefwechsel zwischen C. G. J. JACOBI und P. H. VON FUSS über die Herausgabe der Werke LEONHARD EULERS*, Leipzig 1908 (siehe auch Biblioth. Mathem. 8_3, 1907/8, p. 233–306).

3) So möge in Zukunft die Sammlung der Brüder FUSS kurz bezeichnet werden.

hat es gänzlich davon abgesehen, innerhalb eines Bandes die ENESTRÖMSCHE Numerierung noch durch eine zweite, wie immer sie auch gedacht werden könnte, zu durchkreuzen.

In den *Comment. arithm.* sind die als *Summaria dissertationum* bezeichneten Inhaltsübersichten nicht mitabgedruckt. Nun kann man ja freilich über den Wert dieser Summarien verschiedener Meinung sein; in den meisten Fällen aber geben sie doch rasche und hinreichende Auskunft über den Inhalt der betreffenden Abhandlungen und erweisen sich dadurch im allgemeinen als sehr nützlich. Der *Redaktionsplan für die Eulerausgabe*[1]) hat denn auch ihre Aufnahme ausdrücklich gefordert. Übrigens bieten diese Summarien gelegentlich ganz merkwürdige Überraschungen, wie z. B. das zu der Abhandlung 270, das nicht wohl in einer Eulerausgabe fehlen dürfte.

In einem Briefe an C. G. J. JACOBI vom 8./20. Nov. 1847 macht P. H. FUSS[2]) verschiedene Mitteilungen über die Einrichtung der unter der Presse befindlichen *Comment. arithm.* und sagt dabei: „Im Text haben wir uns mit Hinweisungen auf *frühere* Abhandlungen begnügen müssen, die auch schon Mühe genug kosteten, weil EULER sich selbst immer nur nach dem Gedächtnis, nie genau zitiert.“ Hierzu ist folgendes zu sagen. Den Abhandlungen, die den vorliegenden Band füllen, sind in den *Comment. arithm.* alles in allem 16 Fußnoten beigefügt, die nicht einmal sämtlich als eigentliche Hinweisungen auf frühere Arbeiten EULERS gelten können. Daß so spärliche Notizen aber ganz und gar nicht ausreichen, um den Zusammenhang zwischen den einzelnen Abhandlungen erkennen zu lassen, zeigt schon ein flüchtiger Vergleich mit den Anmerkungen des vorliegenden Bandes, deren Zahl noch leicht hätte vergrößert werden können. Im Hinblick auf die enorme Produktivität EULERS — weist doch das ENESTRÖMSCHE Verzeichnis nicht weniger als 866 Nummern auf — hat es denn auch das Redaktionskomitee als eine wichtige und dankbare Aufgabe bezeichnet, nicht nur den eigenen Hinweisungen EULERS auf frühere Arbeiten, selbst wenn sie in ganz unbestimmter oder gar fehlerhafter Form gehalten sein sollten, prüfend nachzugehen und die Zitate zu vervollständigen oder in Ordnung zu bringen, sondern überhaupt nach Möglichkeit dafür zu sorgen, daß die Beziehungen zwischen den einzelnen Arbeiten aufgedeckt und diese dadurch zu höheren Einheiten vereinigt werden. Dazu genügt oft eine kurze Notiz, wobei man auch vor Hinweisungen auf spätere Arbeiten EULERS nicht zurückschrecken darf.[3])

Hinweisungen auf Arbeiten anderer Autoren enthalten die Anmerkungen der *Comment. arithm.* gar keine. Aber auch solche sind in dem *Redaktionsplan für die Eulerausgabe* vorgesehen

1) Jahresber. d. Deutschen Mathem.-Verein. 19, 1910, Zweite Abt., p. 94.

2) Siehe P. STÄCKEL und W. AHRENS, *Der Briefwechsel* etc., p. 40.

3) Durch geeignete Ergänzungen habe ich übrigens dieser und ähnlichen Aufgaben auch noch im Vorwort Rechnung zu tragen gesucht.

und mit Recht. So gibt es, um nur ein Beispiel herauszugreifen, nur wenige arithmetische Abhandlungen Eulers, in denen nicht der Name Fermat oder Diophant vorkäme, und man kann ohne weiteres sagen, daß überhaupt die meisten seiner arithmetischen Untersuchungen in den Arbeiten dieser beiden großen Zahlentheoretiker wurzeln. Genauere Angaben aber über die Stellen, auf die sich Euler gerade bezieht, findet man bei ihm nur selten, so wünschenswert sie auch erscheinen. Diese Lücken auszufüllen habe ich mir im vorliegenden Bande zur ganz besonderen Aufgabe gemacht und ich hoffe, daß es mir gelungen sei, alle die Fäden, die Euler speziell mit Fermat und Diophant verbinden, entwickelt und klargelegt zu haben. Die Arbeit gestaltete sich dadurch etwas umständlicher, daß neben den alten Ausgaben, die Euler zur Verfügung hatte, auch die modernen zu berücksichtigen waren, die mit jenen nicht überall übereinstimmen. Da aber die alten Ausgaben selten sind, so ist durch diese doppelte Behandlung dem Leser doch vielleicht ein Dienst erwiesen worden. Unserem Redaktionsplane entsprechend führen wir ja auch Zitate, die sich auf Eulersche Schriften beziehen, zugleich in die neue Ausgabe über.

Wenn nun auch ihrer großen Bedeutung wegen die Arbeiten von Fermat und Diophant im Vordergrunde stehen und daher eine besonders eingehende Berücksichtigung verlangten, so werden doch in den Abhandlungen des vorliegenden Bandes außerdem noch sehr viele andere Mathematiker, teils mit Namen, teils auch nur andeutungsweise (siehe z. B. p. 307 und 431) erwähnt, wie Bachet, Descartes, Euklid, Frénicle, Lahire, Naudé, Rudolff, Sauveur, Schooten, Stifel, Vieta, Wallis, Wolf u. a., deren Arbeiten mit Eulerschen Untersuchungen zusammenhängen und daher ausfindig gemacht und genau zitiert werden mußten — denn Euler hat nicht nur sich selbst, sondern auch fremde Autoren „immer nur nach dem Gedächtnis, nie genau zitiert“. Wie bei Fermat und Diophant so durfte auch hier keine Mühe gescheut und keine Anmerkung unterlassen werden, die geeignet war, die Stellung und die Bedeutung der Eulerschen Schöpfungen in der Entwickelung der Zahlentheorie hervortreten zu lassen.

Zu diesen historischen Notizen gesellten sich sodann noch Hinweisungen auf Eulers Briefwechsel, der in der dritten Serie unserer Ausgabe erscheinen soll. Im wesentlichen handelte es sich dabei um Briefe, die in der *Correspondance math. et phys. publiée par P. H. Fuss*, St.-Pétersbourg 1843, veröffentlicht sind, dann aber auch um solche, die sich in dem noch unveröffentlichten wertvollen Manuskriptenmaterial befinden, das die Kaiserliche Akademie der Wissenschaften in St. Petersburg dem Redaktionskomitee in so liberaler und dankenswerter Weise zur Verfügung gestellt hat. Der Briefwechsel Eulers ist auch noch dadurch von besonderer Wichtigkeit, daß er in vielen Fällen die Abfassungszeit der betreffenden Arbeiten genauer zu bestimmen erlaubt und überdies gelegentlich Aufschluß gibt über Erscheinungen, die sonst schwer verständlich wären (siehe z. B. die Anmerkungen p. 520 und 530).

Abgesehen von jenen Briefen konnten auch noch weitere Manuskripte der Petersburger Akademie für den vorliegenden Band verwendet werden. Diese Manuskripte, unter denen sich auch zwei bisher unveröffentlichte Summarien (zu den Abhandlungen 26 und 29) befinden, haben an vielen Stellen Verbesserungen und Ergänzungen der gedruckten Texte ermöglicht. Da aber alle Änderungen dieser Art durch besondere Anmerkungen gekennzeichnet worden sind, so kann ich darauf verzichten, sie hier einzeln namhaft zu machen.

Zu den Petersburger Handschriften gehören auch die 13 Notizbücher EULERS[1]), die sich über die Jahre 1726 bis 1783*, also fast über seine ganze Lebenszeit, erstrecken und von denen bisher nur die drei letzten (aus den Jahren 1767 bis 1783) unter dem Namen *Adversaria mathematica* bekannt waren. Auszüge (*Fragmenta*) daraus sind in den *Opera postuma* veröffentlicht. Es versteht sich von selbst, daß nicht nur diese *Adversaria*, sondern überhaupt alle Notizbücher daraufhin untersucht werden müssen, was davon der Aufnahme in die Eulerausgabe wert erscheint. Speziell arithmetische Notizen werden im Bande I_5 untergebracht werden.

Ganz ausnahmsweise und nur an ganz besonders wichtigen Stellen ist in den Anmerkungen des vorliegenden Bandes auch auf spätere Autoren Bezug genommen worden. Abgesehen von Verfassern historischer Arbeiten handelt es sich dabei im wesentlichen um LAGRANGE, dessen Untersuchungen mehrfach da einsetzen, wo EULER selbst erklärt, mit den Beweisen nicht zustande gekommen zu sein, und um JACOBI. Es ist aber wohl anzunehmen, daß auch die umfangreiche Anmerkung p. 191, die der Stelle gilt, wo bei EULER zum ersten Male eine ϑ-Reihe auftritt, dem Leser nicht unwillkommen sein werde. Übrigens ist im Art. 16 des Redaktionsplanes ausdrücklich darauf hingewiesen, daß Stellen von solchem Range nicht mit Stillschweigen übergangen werden sollen.

Wichtiger als Reichhaltigkeit an historischen Notizen ist Korrektheit einer Ausgabe. Damit kehre ich wieder zu den *Comment. arithm.* zurück, aber leider auch zu einer unerfreulichen Sache. In dem schon erwähnten Briefe von FUSS an JACOBI heißt es: „Mein Bruder steht mir treulich bei, und die Ausgabe wird nicht nur sauber und würdig, sondern auch korrekt.“ Die Korrektheit muß zugestanden werden, aber nur in dem Sinne, daß im wesentlichen die Editio princeps wortgetreu, um nicht zu sagen mechanisch, abgedruckt wurde. Wer indessen bedenkt, wie viel, wie enorm viel EULER produziert hat und wie rasch er daher produziert haben muß, wird es nur allzu begreiflich finden, daß sich bei der Redaktion dieser zahllosen Arbeiten Flüchtigkeitsfehler der verschiedensten Art fast mit Notwendigkeit haben einschleichen müssen. Der Größe EULERS tut das keinen Eintrag, aber ein Herausgeber ist deswegen nicht der Verpflichtung enthoben, die Fehler zu verbessern,

1) Siehe G. ENESTRÖM, *Bericht an die Eulerkommission der Schweizerischen naturforschenden Gesellschaft über die EULERSCHEN Manuskripte der Petersburger Akademie*, Jahresber. d. Deutschen Mathem.-Verein. 22, 1913, Zweite Abt., p. 191.

und dies um so weniger, als man weiß, daß auch gewichtige Fehler vorkommen, die gar nicht von EULER herrühren, sondern durch Nachlässigkeit bei der Besorgung der Drucklegung entstanden sind.[1]) Leider ist in den *Comment. arithm.* nur ganz ausnahmsweise dieser Forderung Genüge geleistet. In den weitaus meisten Fällen sind die Fehler des Originals, theoretische Fehler, Rechenfehler, Druckfehler bis herab zur sinnlosesten Interpunktion getreu abgedruckt worden. Bei aller Pietät und bei aller dankbaren Anerkennung der großen Verdienste, die sich die Brüder FUSS um die Herausgabe der Werke EULERS erworben haben, darf dies nicht verschwiegen werden. Ich habe in den Anmerkungen des vorliegenden Bandes eine Reihe von Belegen mitgeteilt, aber nur solche, die besonders erwähnenswert schienen. Die Zahl würde unverhältnismäßig viel größer ausfallen, wenn man die vielen Stellen mitzählen wollte, an denen ich entweder stillschweigend oder doch ohne Erwähnung der *Comment. arithm.* korrigiert habe.

Ich hoffe, daß nicht nur der vorliegende Band, sondern überhaupt unsere Eulerausgabe, als korrekt in einem höheren Sinne befunden werde. Dafür dürfte wenigstens die Einrichtung unseres Arbeitsplanes einige Garantie bieten. Denn nicht nur wird die vom Herausgeber hergestellte Druckvorlage von zwei Redaktoren kontrolliert, es werden auch von jedem Bogen mindestens drei, oft aber vier und noch mehr Korrekturen gelesen und jede dieser Korrekturen wird nicht nur vom Herausgeber, sondern auch von jedem der drei Redaktoren und außerdem noch von einem klassischen Philologen für die lateinischen, von einem Romanisten für die französischen Texte besorgt. Der Betrieb ist freilich nicht einfach, aber die aufgewandte Mühe wird sich hoffentlich lohnen.

Wenden wir uns nun zu einer kurzen Übersicht über den Inhalt der 26 Abhandlungen des vorliegenden Bandes.

Gleich die erste Abhandlung 26, die EULER 1732, also 25jährig, der Petersburger Akademie vorgelegt hat, läßt den Meister erkennen und eröffnet trotz ihrer Kürze weitreichende Perspektiven. Das Wichtigste darin ist die Widerlegung der Behauptung von FERMAT, alle Zahlen der Form $2^{2^m}+1$ seien Primzahlen. Mit diesem Satze, der für $m=0, 1, 2, 3, 4$ richtig ist, hatte sich EULER auf Anregung von CHR. GOLDBACH[2]) schon seit 1729, wenn auch lange vergeblich, beschäftigt. Erst als er erkannt hatte, daß die Zahlen $2^{2^m}+1$, falls sie nicht

---

1) Siehe hierüber den Auszug aus EULERS Brief an den damaligen Sekretär der Petersburger Akademie G. F. MÜLLER vom 27. Juli 1762, den G. ENESTRÖM in seinem *Verzeichnis* (Lief. 2, Leipzig 1913, p. 214) mitteilt.

2) Siehe die Briefe 2—8 in *Correspondance math. et phys. publiée par P. H. Fuss*, St. Pétersbourg 1843, t. I, p. 8—34.

prim sind, nur Divisoren von der Form $2^{m+1}n+1$ besitzen können, was allerdings erst in der Abhandlung 134 bewiesen wird, konnte er sich an die Prüfung der Zahl $2^{32}+1=4294967297$ heranwagen und nun fand er mit verhältnismäßig geringer Mühe, daß sie durch 641 teilbar ist.[1]) Der Rest der Abhandlung beschäftigt sich mit Beispielen der Teilbarkeit von Zahlen der Form 2^p-1 und sodann, freilich ohne Beweis, mit dem FERMATSCHEN Satze von der Teilbarkeit der Zahlen $a^{p-1}-1$, den EULER auch in der Form ausspricht, es sei stets $a^{p-1}-b^{p-1}$ durch p teilbar.[2]) Die Sätze, die er, wiederum ohne Beweis, hinzufügt, zeigen, daß er schon damals im Besitze von wesentlichen Verallgemeinerungen dieses FERMATSCHEN Satzes war, Verallgemeinerungen, die ihren Abschluß freilich erst viel später in dem berühmten Satze fanden, den wir jetzt in der Form $a^{\varphi(k)}\equiv 1 \pmod{k}$ schreiben und der in der Abhandlung 271 bewiesen ist.

In der folgenden Abhandlung 29 vom Jahre 1733 wendet sich EULER zu der Lösung DIOPHANTISCHER Probleme, insbesondere zu der Auflösung der Gleichung

$$ax^2+bx+c=y^2$$

in ganzen Zahlen. Er zeigt, daß, wenn man eine Lösung kennt, hieraus mit Hülfe der Gleichung $ap^2+1=q^2$ unendlich viele Lösungen gefunden werden können und daß diese durch eine einfache Rekursionsformel miteinander verbunden sind. In einer Tabelle fügt er für alle nichtquadratischen Zahlen $a=2, \ldots 68$ die kleinsten Lösungen dieser FERMATSCHEN Gleichung $ap^2+1=q^2$ hinzu, von der wir heute wissen, daß sie von EULER nur irrtümlicher Weise mit dem Namen PELL in Verbindung gebracht worden ist. Am Schlusse der Abhandlung wird gezeigt, wie man mit Hülfe dieser Untersuchungen alle Trigonalzahlen und andere Polygonalzahlen finden kann, die zugleich Quadrate sind.

Mit der Abhandlung 29 ist aufs engste die Abhandlung 279 aus dem Jahre 1758 verbunden, die den Schluß des Bandes bildet. Auch hier handelt es sich um die Gleichung $ax^2+bx+c=y^2$, aber EULER geht jetzt wesentlich über die früheren Untersuchungen hinaus, indem er zu den Rekursionsformeln, die für die Lösungen gelten, auf Grund der Theorie der rekurrenten Reihen und der Partialbruchzerlegung, wie er sie in der *Introductio* (1748) entwickelt hatte, auch die Darstellung in independenter Form hinzufügt. Ausführlicher werden

1) Daß EULER tatsächlich auf diesem Wege den FERMATSCHEN Satz widerlegt hat, sagt er selbst in § 32 der Abhandlung 134. Er war also spätestens 1732 im Besitze des Satzes von den Divisoren der Zahlen $2^{2^m}+1$. Ob er auch damals schon einen Beweis dafür hatte, geht daraus noch nicht hervor. Er fand den Beweis aber spätestens 1743, wie sich aus einem Briefe an GOLDBACH ergibt (siehe die Anmerkung 3 p. XVII).

2) Von den 11 Zahlen, die EULER bei diesem Anlaß als *vollkommene* bezeichnet, sind nach G. ENESTRÖM (*Encycl. d. sc. math.*, t. I, vol. 3, fasc. 1, p. 55) die zwei letzten ($n=41$ und $n=47$) zu streichen.

sodann die Formeln $\alpha x^2+\gamma$ untersucht, weil sich auf diese die allgemeineren leicht zurückführen lassen. Bei der Untersuchung, welche Zahlen dabei für γ zulässig sind, wird EULER auf das „theorema elegantissimum" geführt, daß, wenn sich p und q in der Reihe der zulässigen Zahlen befinden, auch ihr Produkt pq darin enthalten ist. Anwendungen und Beispiele bilden den Schluß der Abhandlung. EULER konnte natürlich nicht wissen, daß das Theorem, dem er mit Recht eine so große Bedeutung beigelegt hat, schon den alten Indern bekannt gewesen war.

In der Abhandlung 36, deren Exhibitionsdatum unbekannt ist und die ENESTRÖM daher in seinem *Verzeichnis* (zweite Abt.) unter dem Druckjahre 1740 aufgeführt hat, — sie ist aber wohl viel früheren Datums — löst EULER die Aufgabe, Zahlen zu finden, die durch gegebene Zahlen dividiert gegebene Reste zurücklassen. Er entwickelt zunächst eine einfache Regel für zwei Divisoren und zeigt sodann, wie sich der Fall von beliebig vielen Divisoren hierauf zurückführen läßt, vorausgesetzt, daß die Aufgabe überhaupt lösbar ist.[1])

Die folgende Abhandlung 54, die aus dem Jahre 1736 stammt, aber erst 1741 veröffentlicht wurde, bringt den ersten Beweis EULERS für den FERMATSCHEN Satz von der Teilbarkeit der Zahlen $a^{p-1}-1$ oder, wie EULER auch sagt, der Zahlen a^p-a durch die Primzahl p. Der Beweis stützt sich auf den binomischen Satz und die Eigenschaften der Binomialkoeffizienten, ist also eigentlich nicht zahlentheoretischer Natur. Die Wichtigkeit des FERMATSCHEN Satzes läßt es verstehen, daß EULER später, in den Abhandlungen 134 und 262, noch zwei weitere Beweise hinzugefügt hat, bis es ihm dann gelang, in der Abhandlung 271 den schon erwähnten verallgemeinerten FERMATSCHEN Satz $a^{\varphi(k)}\equiv 1 \pmod{k}$ zu begründen. Daß EULER von dem LEIBNIZSCHEN Beweise des FERMATSCHEN Satzes keine Kenntnis haben konnte, bedarf kaum der Erwähnung.

Im Zeichen FERMATS steht auch die im Jahre 1738 verfaßte Abhandlung 98, in der zum ersten Male bei EULER ein spezieller Fall des sogenannten großen FERMATSCHEN Satzes auftritt, des Satzes von der Unmöglichkeit, die Gleichung $x^n+y^n=z^n$ für $n>2$ durch ganze Zahlen zu befriedigen. Es handelt sich hier um $n=4$[2]) und für diesen Fall hatte bereits 1676 FRÉNICLE DE BESSY den Beweis geführt, daß in ganzen Zahlen weder die Summe noch die Differenz zweier Biquadrate ein Quadrat sein kann, woraus dann von selbst folgt, daß solche Ausdrücke auch kein Biquadrat sein können. Die Abhandlung von FRÉNICLE ist nur eine weitere Ausführung einer der berühmten Anmerkungen, die FERMAT an den Rand seines Handexemplares von BACHETS Ausgabe der *Arithmetik* DIOPHANTS geschrieben hat und die

1) Siehe hierzu die Bemerkungen von G. ENESTRÖM, Biblioth. Mathem. 9_3, 1908/9, p. 331 und 339.

2) EULER hat bekanntlich auch die Unmöglichkeit der Gleichung $x^3+y^3=z^3$ bewiesen. Siehe die Anmerkung p. XXXIII.

von seinem Sohne S. FERMAT in der Toulouser Ausgabe DIOPHANTS vom Jahre 1670 abgedruckt worden sind. Sie spielen bei EULER und daher auch in unserem Bande eine große Rolle. Im vorliegenden Falle handelt es sich um die Randbemerkung, die FERMAT an den Kommentar von BACHET zur letzten Aufgabe des sechsten Buches angeschlossen hat und wonach die Fläche eines rechtwinkligen Dreiecks, dessen Seiten rationale Zahlen sind, keine Quadratzahl sein könne; hieraus ergeben sich dann leicht jene Sätze über die Summe und die Differenz zweier Biquadrate. Der von FRÉNICLE geführte Beweis folgt genau den Andeutungen, die FERMAT seiner Randbemerkung hinzugefügt hat, und er stützt sich insbesondere auf die schon im Mittelalter bekannte und benutzte Methode[1]), die FERMAT Methode der unbegrenzten Abnahme — *la descente infinie* ou *indéfinie* — nennt. Dieser selben Methode bedient sich nun auch EULER, um seinerseits die Unmöglichkeit der Gleichung $a^4 \pm b^4 = c^2$ zu beweisen, aber ohne von der geometrischen Einkleidung des Satzes Gebrauch zu machen. Im Prinzip ist daher der EULERSCHE Beweis nicht wesentlich verschieden von dem, den FRÉNICLE gegeben hat. Dafür fügt aber EULER noch eine Reihe verwandter Sätze hinzu, die sich bei FRÉNICLE nicht finden, indem er zunächst von einer großen Zahl von Formeln, die sich aus Biquadraten zusammensetzen, wie z. B. $ma^4 \pm m^3b^4$, $2ma^4 \pm 2m^3b^4$ u. a., zeigt, daß sie nicht Quadrate sein können. Daran schließt sich der Beweis des von FERMAT ebenfalls in einer Randbemerkung ausgesprochenen Satzes, daß keine Trigonalzahl außer 1 ein Biquadrat sei, sowie des Satzes, daß außer 8 kein Kubus um die Einheit vermehrt zu einem Quadrat gemacht werden könne.

Die Abhandlung 98 ist die erste, in der die Methode der unbegrenzten Abnahme bei EULER auftritt. FERMAT selbst hatte auf diese Art der Beweisführung große Hoffnungen gesetzt und wunderbare Fortschritte in der Arithmetik (miros in Arithmeticis progressus) von ihr erwartet. Diese Hoffnungen sind auch nicht getäuscht worden, denn gerade EULER hat sich der FERMATSCHEN Methode bei einer Reihe von Beweisführungen mit bestem Erfolge bedient, wie auch die Abhandlungen 228 (§ 22), 256 (§ 42), 272 (§ 29) dieses Bandes zeigen. Wir kommen darauf zurück.

Mit der kleinen Abhandlung 100, die 1747 in den Nova acta eruditorum erschien, betritt EULER ein ganz anderes Gebiet der Zahlentheorie, nämlich die Theorie der Divisorensummen, zu der in diesem Bande auch noch die Abhandlungen 152, 175, 243, 244 gehören. Speziell die Abhandlungen 100 und 152 gelten der Theorie der befreundeten Zahlen. Die erste, nur drei Seiten umfassende Abhandlung 100 besteht, abgesehen von einigen historischen Bemerkungen über DESCARTES und SCHOOTEN, im wesentlichen aus einer Tabelle von 30 Paaren befreundeter Zahlen, von denen sich freilich eines als unrichtig erwiesen hat. Vor

1) Siehe hierzu die Bemerkungen von G. ENESTRÖM, Biblioth. Mathem. 14_3, 1913/4, p. 347.

EULER waren nur drei dieser Paare bekannt gewesen. Die Abhandlung 152[1]), die 1750 in den *Opuscula varii argumenti* veröffentlicht, aber vermutlich vor 1747 verfaßt wurde[2]), ist mit 77 Seiten die umfangreichste des ganzen vorliegenden Bandes. Nach den ersten grundlegenden Sätzen über die Divisorensummen stellt EULER eine große Tabelle auf, in der er für alle Primzahlen $n < 1000$ die Divisorensummen $\int n$, $\int n^2$ und $\int n^3$ angibt, und zwar in Primfaktoren ausgedrückt; für die kleineren Primzahlen bis zu 23 geht er noch wesentlich höher. Bei der Herstellung dieser Tabelle hat EULER eine allerdings lange nicht so weit reichende Vorarbeit von WALLIS[3]) benutzt. Für die Auffindung befreundeter Zahlen setzt er nun einen gemeinsamen Divisor a voraus und entwickelt in fünf Problemen verschiedene Methoden, befreundete Zahlen am und an zu gewinnen, wobei sich das fünfte, bei dem für gegebene Formen von m und n nach einem passenden Teiler a gefragt wird, als besonders ergiebig erweist. Zum Schlusse gibt EULER eine Tabelle von 61 Paaren befreundeter Zahlen, von denen 41 in der Abhandlung selbst gewonnen worden sind, während die anderen 20 ohne weitere Begründung mitgeteilt werden. Von diesen 61 Paaren sind aber zwei verbesserungsbedürftig und eines ist als verfehlt zu streichen. In der Tabelle sind auch die Paare der Abhandlung 100, mit Ausnahme von zweien, enthalten und so ergibt sich, daß EULER alles in allem genau 62 Paare befreundeter Zahlen mitgeteilt, also zu den dreien, die vor ihm bekannt waren, 59 neue hinzugefügt hat.

Da die Besprechung der bereits genannten Abhandlungen 175, 243, 244 besser später erfolgt, gelangen wir zu der Abhandlung 134 aus dem Jahre 1747, die um so bemerkenswerter ist, als EULER hier zum ersten Male die Theorie der Reste, insbesondere der quadratischen, berührt, in der er so Großes geleistet hat. Die Abhandlung beginnt mit einem zweiten Beweise des FERMATSCHEN Satzes. Wie der frühere (Abhandlung 54) beruht auch dieser Beweis auf dem binomischen Satze; nur hat er im Gegensatze zu jenem einen mehr deduktiven Charakter, indem er von der Teilbarkeit des allgemeinen Ausdrucks $(a+b)^p - a^p - b^p$ durch die Primzahl p ausgeht. Aus dem FERMATSCHEN Satze beweist dann EULER, daß a^2+b^2 (sofern a und b teilerfremd sind) durch keine Primzahl der Form $4n-1$ teilbar ist, also überhaupt keine Divisoren dieser Form besitzen kann. Daß a^2+b^2 selbst niemals von der Form $4n-1$ sein kann, war freilich längst bekannt und ist leicht einzusehen. Auch daß a^2+b^2 nicht einmal Teiler dieser Art zuläßt, war, wie EULER selbst hervorhebt,

---

1) Ich habe über diese Abhandlung an anderem Orte ausführlicher berichtet. Siehe **Biblioth. Mathem.** 14_3, 1913/4, p. 351.

2) Siehe hierüber die Bemerkungen von G. ENESTRÖM, **Biblioth. Mathem.** 12_3, 1912/3, p. 172, und 14_3, 1913/4, p. 351.

3) Siehe J. WALLIS, *A Treatise of Algebra*, London (in der Anmerkung p. 104 steht irrtümlich Oxford) 1685, Additional Treatise IV, p. 140—144.

nicht neu[1]), aber ein Beweis für diesen wichtigen Satz war doch bisher nicht bekannt gewesen[2]), wenn auch FERMAT in seinem berühmten Briefe an ROBERVAL (siehe die Anmerkung p. 70) behauptet hatte, einen solchen gefunden zu haben.

Nachdem Euler gezeigt hatte, daß alle ungeraden Teiler von a^2+b^2 von der Form $4n+1$ sind, zeigte er, daß die ungeraden Teiler von a^4+b^4 in $8n+1$, die von a^8+b^8 in $16n+1$ und allgemein alle ungeraden Teiler von $a^{2^m}+b^{2^m}$ in der Form $2^{m+1}n+1$ enthalten sein müssen.[3]) Als wichtige Anwendung ergab sich ihm dann die Folgerung, daß $2^{32}+1$ nur Teiler der Form $64n+1$ besitzen kann, und so gelang es ihm, wie wir gesehen haben, die FERMATSCHE Behauptung, alle Zahlen $2^{2^m}+1$ seien Primzahlen, zu widerlegen.

Von besonderer Wichtigkeit sind nun die folgenden Theoreme 10—16, weil sie für die Theorie der quadratischen und der höheren Reste bereits eine grundlegende Bedeutung besitzen. Unter Benutzung der von EULER selbst in seiner Abhandlung 242 eingeführten Terminologie heißt z. B. das Theorem 11: Ist a (quadratischer) Rest der Primzahl $p=2m+1$, so ist $a^{\frac{p-1}{2}}-1$ durch p teilbar," oder moderner ausgedrückt, so ist $a^{\frac{p-1}{2}}\equiv+1$ (mod. p). Das Theorem 12 gibt den entsprechenden Satz für die kubischen Reste und allgemein sagt das Theorem 13: Ist $a\equiv f^n$ (mod. $p=mn+1$), so ist $a^{\frac{p-1}{n}}\equiv+1$ (mod. p). Die Umkehrung dieses Satzes zu beweisen, war EULER, wie er mit der ihm eigenen Offenheit eingesteht, damals noch nicht in der Lage. Er hat den Beweis aber später in der Abhandlung 262 gegeben und damit zugleich das vollständige Kriterium entwickelt, das den quadratischen *Charakter* einer Zahl bestimmt. Wir werden davon noch zu sprechen haben. Die Theoreme 14—16 endlich verallgemeinern das Theorem 13, indem sie von der durch $p=mn+1$ teil-

1) Es scheint sogar, daß schon DIOPHANT diesen Satz gekannt habe (siehe die Anmerkung p. 70). Wenigstens war das die Ansicht FERMATS, der die betreffende stark verstümmelte Stelle bei DIOPHANT (V, 12) in diesem Sinne restauriert hat.

Ich möchte noch darauf aufmerksam machen, daß die Bezeichnung V, 12 der Numerierung von BACHET entspricht, die auch WERTHEIM beibehalten hat. TANNERY hat anders numeriert und so ist bei ihm (I, p. 332) die Aufg. 12 des fünften Buches als Aufg. 9 bezeichnet. Um Mißverständnisse zu vermeiden, habe ich in den folgenden Anmerkungen allemal beide Numerierungen mitgeteilt (siehe die Anmerkung p. 404).

2) Die Abhandlung 134 stammt aus dem Jahre 1747 und wurde 1748 der Petersburger Akademie vorgelegt; EULER hatte aber seinen Beweis schon am 6. März 1742 GOLDBACH brieflich mitgeteilt, *Correspondance math. et phys.* I, p. 114.

3) Diesen Satz hatte EULER am 15. Oktober 1743 GOLDBACH mitgeteilt, *Correspondance math. et phys.* I, p. 258. Danach ist eine Bemerkung von G. ENESTRÖM, Biblioth. Mathem. 7_3, 1906/7, p. 308, zu vervollständigen (siehe auch die Anmerkung p. XIII).

baren Differenz $f^n - a$ zunächst zu $f^n - a g^n$ und sodann zu der Differenz $a f^n - b g^n$ übergehen, aus deren Teilbarkeit die Teilbarkeit von $a^n - b^n$ gefolgert wird[1])

Wiederum einem anderen Zweige der Zahlentheorie gehört die Abhandlung 158 vom Jahre 1741 an. Wir haben schon von ihr gesprochen als der einzigen dieses Bandes, die nicht in die *Comment. arithm.* aufgenommen worden ist — vermutlich wegen ihres Titels, der die Abhandlung der Kombinatorik zuweist. Zu dieser müßten dann aber überhaupt alle Abhandlungen gerechnet werden, die sich auf die *Partitio numerorum* beziehen. Die ersten 16 Paragraphen der Abhandlung 158 sind freilich rein kombinatorischer Natur. Aus gegebenen Größen a, b, c, d etc. bildet EULER zunächst die Summe, sodann die Summe der Produkte zu je zweien, die zu je dreien etc. und erhält dadurch, je nachdem Gleichheit der Faktoren gefordert, ausgeschlossen oder zugelassen wird, drei Serien von Kombinationen, zwischen denen nun Beziehungen aufgesucht werden. Insbesondere werden analytische Funktionen einer Variabeln z in Form von unendlichen Reihen und Produkten eingeführt, aus deren Entwickelung jene Kombinationen als Koeffizienten hervorgehen. Aber diese Untersuchungen sind nur Vorbereitungen zur Lösung der zahlentheoretischen Aufgaben, denen der größere Teil der Abhandlung gewidmet ist. Indem nämlich EULER für a, b, c, d etc. speziell die Potenzen n, n^2, n^3, n^4 etc. wählt, erhält er für jene Kombinationen Entwickelungen nach Potenzen von n, in denen die Koeffizienten, die aus einfachen Rekursionsformeln hervorgehen, angeben, auf wieviel verschiedene Arten die zugehörigen Exponenten in eine vorgeschriebene Anzahl von Teilen zerlegt werden können, wobei das eine Mal die Gleichheit der Teile ausgeschlossen, das andere Mal aber zugelassen wird. Diese beiden Probleme waren EULER im Jahre 1740 von dem Berliner Akademiker PHILIPP NAUDÉ (1684—1745[2])), dem Jüngeren, vorgelegt worden. EULER zeigt nun noch, daß die beiden Aufgaben wegen der erwähnten Beziehungen zwischen jenen Kombinationen in engem Zusammenhange stehen, sodaß die Lösung der zweiten leicht auf die der ersten zurückgeführt werden kann.

Der Schluß der Abhandlung 158 bietet noch eine besondere Überraschung: das erste Auftreten einer ϑ-Reihe bei EULER. Die aus der Entwickelung[3]) des unendlichen Produktes

$$(1-n)(1-n^2)(1-n^3)(1-n^4)\cdots$$

entspringende Reihe

$$1-n-n^2+n^5+n^7-n^{12}-n^{15}+\cdots,$$

---

1) Dieser Satz findet sich schon in einem Briefe EULERS an GOLDBACH vom 16. Februar 1745, *Correspondance math. et phys.* I, p. 311.

2) In der Anmerkung p. 178 steht irrtümlich 1747.

3) Der in der Anmerkung p. 191 zitierte Brief, den DANIEL BERNOULLI am 28. Jan. 1741 an EULER gerichtet hat und in dem bereits diese Entwickelung erwähnt wird, ist nach den Protokollen der Petersburger Akademie die Antwort auf einen Brief EULERS vom 30. Nov. 1740, der leider verloren gegangen ist.

die auch noch in späteren Abhandlungen EULERS eine wichtige Rolle spielt, hängt mit der *Partitio numerorum* insofern zusammen, als die zu ihr reziproke Reihe die Frage beantwortet, auf wieviel verschiedene Arten überhaupt eine Zahl in Teile zerlegt werden könne.

Die Abhandlung 158 ist in zweierlei Hinsicht besonders beachtenswert. Erstens wird durch sie, von vereinzelten Vorarbeiten abgesehen (siehe die Anmerkungen p. 257 und 258), die Lehre von der *Partitio numerorum* eigentlich erst begründet. Zweitens aber enthält sie, wenigstens bei EULER, das erste Beispiel für die Benutzung von Hülfsmitteln der höheren Analysis zu zahlentheoretischen Untersuchungen. Welch reiche Früchte späterhin der mathematischen Wissenschaft aus der Verbindung dieser beiden Disziplinen erwachsen sind, braucht hier nicht weiter ausgeführt zu werden.

EULER hatte die Abhandlung 158 schon am 6. April 1741 der Petersburger Akademie vorgelegt, gedruckt aber wurde sie erst 1751. Inzwischen war 1748 seine *Introductio* erschienen, deren 16. Kapitel ebenfalls der *Partitio numerorum* gewidmet ist. Am 26. Januar 1750[1]) legte nun EULER der Petersburger Akademie die große Abhandlung 191 *De partitione numerorum* vor, die 1753 veröffentlicht wurde. Mit dieser haben wir uns jetzt zu befassen. Ähnlich wie in der Abhandlung 158, aber direkter, löst EULER zunächst die beiden Probleme, die ihm von NAUDÉ gestellt worden waren, indem er sich wieder der früheren Produktentwickelungen bedient. Dann aber vollzieht er eine wichtige Reduktion, die auch schon in der *Introductio* auftritt, indem er die beiden Probleme auf ein drittes zurückführt, nämlich auf die Aufgabe, anzugeben, auf wieviel verschiedene Arten irgend eine Zahl n aus den Zahlen 1, 2, 3, ... m durch Addition gebildet werden könne. Bezeichnet man diese Anzahl mit $n^{(m)}$, so gibt zugleich die Zahl $\left(n-\frac{m(m+1)}{2}\right)^{(m)}$ an, auf wieviel Arten die Zahl n in m verschiedene Teile zerlegt werden kann, während $(n-m)^{(m)}$ sagt, wie oft sich n überhaupt in m Teile, seien es gleiche oder ungleiche, teilen läßt. Für die Herstellung dieser Zahlen $n^{(m)}$ werden einfache und sehr übersichtliche Rechnungsvorschriften entwickelt, die lediglich auf fortgesetzter Addition beruhen und gegenüber der *Introductio* einen nicht unwesentlichen Fortschritt bedeuten.

Nunmehr wendet sich EULER zu einem vierten Problem, indem er m beliebig groß werden läßt. Mit $n^{(\infty)}$ bezeichnet er demgemäß, wie oft sich n überhaupt ohne Einschränkung aus ganzen Zahlen zusammensetzen läßt. Diese Aufgabe hatte EULER am Schlusse der Abhand-

1) Siehe indessen auch die Anmerkung p. 289, in der die Entstehung der Abhandlung 191 in das Jahr 1745 verlegt worden ist. Die Wahl dieser Zahl 1745 als Beispiel dürfte wohl kaum auf einem Zufall beruhen. Auch bei EULERS Sohne JOHANN ALBRECHT stößt man bei Zahlenbeispielen auf das Jahr der Abfassung. Siehe das Exempel in § 5 der Abhandlung A_9 (des ENESTRÖMSCHEN Verzeichnisses): *ALBRECHT EULERS Beantwortung einiger Arithmetischen Fragen*, Abhandl. der Churfürstl.-baier. Akad. der Wiss. 2, 1764, II, p. 3; *LEONHARDI EULERI Opera omnia*, series I, vol. 3.

lung 158 gerade noch gestreift. Sie hatte ihn, wie wir gesehen haben, zur Entwickelung des Produktes $(1-x)(1-x^2)(1-x^3)\cdots$ veranlaßt, die zu jener ϑ-Reihe geführt hatte. Die Entwickelung des reziproken Produktes enthält in ihren Koeffizienten die Lösung der gestellten Aufgabe. Mehr bietet auch die *Introductio* nicht zu dieser Frage. In der vorliegenden Abhandlung aber entwickelt EULER eine Reihe wichtiger Formeln für $n^{(\infty)}$, unter denen die Gleichung

$$n^{(\infty)} = (n-1)^{(\infty)} + (n-2)^{(\infty)} - (n-5)^{(\infty)} - (n-7)^{(\infty)} + (n-12)^{(\infty)} + (n-15)^{(\infty)} - \dots$$

wegen ihrer Verwandtschaft mit der ϑ-Reihe besonders zu erwähnen ist. Außerdem zeigt er, wie man mit Benutzung der schon berechneten Zahlen $n^{(m)}$, z. B. mit Benutzung von $n^{(20)}$, zu einer stark abgekürzten Berechnung der Zahlen $n^{(\infty)}$ gelangen kann.

Wie in der *Introductio* schließt sich daran die weitere Aufgabe, anzugeben, wie oft sich eine Zahl in ungleiche Teile zerlegen lasse, und es wird gezeigt, daß dies ebenso oft möglich ist, als sich dieselbe Zahl aus nur ungeraden Zahlen, seien es gleiche oder ungleiche, zusammensetzen läßt. Diese Aufgabe leitet daher zu solchen über, bei denen von den Summanden gewisse Qualitäten verlangt werden, z. B. der geometrischen Reihe 1, 2, 4, 8, 16, 32 etc. anzugehören, wobei wiederum Gleichheit der Summanden ausgeschlossen oder auch zugelassen werden kann.

Den Schluß der Abhandlung bildet endlich eine große Tabelle für die Zahlen $n^{(m)}$, die für $n=1,\dots 59$ und für $m=1,\dots 20$ und $m=\infty$ zusammengestellt ist und die zugleich auch ihre Entstehungsweise erkennen läßt. Die entsprechende Tabelle der *Introductio*, die nur die fertigen Zahlen bietet, reicht zwar bis $n=69$, aber dafür auch nur bis $m=11$, ohne die Reihe $m=\infty$ zu enthalten.

Mit der Abhandlung 164, die aus dem Jahre 1747 stammt, aber erst 1751 veröffentlicht wurde und zwar im letzten Bande der alten Commentarii, kehren wir wieder zu einem früheren Thema zurück, das mit der Theorie der quadratischen Reste zusammenhängt. Ihrem Hauptinhalte nach besteht diese Abhandlung aus 59 Sätzen, die ohne Beweis mitgeteilt werden und die sich auf die Divisoren der Zahlen von der Form pa^2+qb^2 beziehen.[1]) Wie EULER später selbst in der Abhandlung 598 sagt, hatte er diese Sätze größten-

1) Es ist schon früher (siehe die Anmerkung p. VII) darauf aufmerksam gemacht worden, daß die aus demselben Jahre 1747 stammende Abhandlung 134 im ersten Bande der neuen Commentarii erschienen ist. Dieser Umstand und die Ähnlichkeit der Titel beider Abhandlungen hat gelegentlich zu Mißverständnissen geführt (siehe die Bemerkungen von G. ENESTRÖM, Biblioth. Mathem. 12_3, 1911/2, p. 266). Zwischen den beiden Abhandlungen 134 und 164 bestehen aber nur wenige Beziehungen, denn von sämtlichen in 164 auftretenden Formen wird in 134 nur die erste, nämlich a^2+b^2, behandelt. Von den andern Formen hat EULER selbst überhaupt nur noch die Form a^2+3b^2 erledigt, aber erst in der Abhandlung 272, während er mit der Form a^2+2b^2,

teils nur durch Induktion gefunden. Um so wichtiger sind daher die hinzugefügten Anmerkungen, die freilich auch nicht überall als beweiskräftig gelten sollen. Dazu gehört namentlich, daß alle Divisoren von a^2+qb^2, abgesehen von 2 und q, in der Form $4qm+\alpha$ enthalten seien und daß sich diese Form für $q=4n-1$ auf $2qm+\alpha$ reduziere; ferner daß pa^2+qb^2 keinen Divisor habe, der nicht zugleich Divisor von a^2+pqb^2 ist, etc. Gegenstand besonderer Untersuchung ist dann die Frage, welche Werte für α zulässig seien, damit $4Nm+\alpha$ Teiler von a^2+Nb^2 sei: α muß quadratischer Rest von $4N$ sein; sind x und y Werte von α, so gilt dies auch für xy und allgemein für $x^\mu y^\nu$ etc., alles Sätze, die EULER erst viel später (in der Abhandlung 242) systematisch behandelt und bewiesen hat.

Die trotz mangelnder Beweise so inhaltsreiche Abhandlung ist ein merkwürdiges Beispiel für die außerordentliche Divinationsgabe EULERS.[1]) Ganz besonders aber zeigt sich das gegen den Schluß der Abhandlung. Denn bei den entsprechenden Untersuchungen der Divisoren von a^2-Nb^2, insbesonders bei der Beantwortung der Frage, welche Werte jetzt für α geeignet seien, damit $4Nm\pm\alpha$ Divisor sei, stellt sich — dem Autor freilich noch unbewußt — das Reziprozitätsgesetz der quadratischen Reste ein, das EULER mit aller Bestimmtheit erst in der Abhandlung 552 ausgesprochen hat. KRONECKER war der erste, der dies bemerkt hatte. Ich habe seine Erklärungen im Wortlaut (siehe die Anmerkung p. 217) mitgeteilt und glaube, nichts weiter hinzufügen zu sollen.

Noch sei hingewiesen auf die vielen interessanten Folgerungen, die EULER an seine Mitteilungen anknüpft und die sich auf Ausdrücke beziehen, die niemals Quadrate sein können. Als Beispiel mag die Formel $4mn-m-n$ gelten, mit der sich EULER schon früh beschäftigt hat (siehe die Anmerkung p. 360).

Die Abhandlung 167, die 1748 zugleich mit der Abhandlung 134 der Petersburger Akademie vorgelegt wurde, gehört zu denen, die zahlentheoretische Untersuchungen in geometrischem Gewande enthalten. Einkleidungen dieser Art waren schon bei DIOPHANT sehr beliebt. Das ganze sechste Buch seiner *Arithmetik* ist mit zahlentheoretischen Aufgaben gefüllt, die sich auf das rechtwinklige Dreieck beziehen, und so spielen derartige Untersuchungen denn auch in den FERMATSCHEN Randbemerkungen eine große Rolle. Ein Beispiel dafür hat uns schon die Abhandlung von FRÉNICLE geboten und auch die vorliegende Abhandlung EULERS verdankt ihre Entstehung einer solchen Randbemerkung. Es sei gleich

---

wie er in der Abhandlung 256 offen zugibt, nicht ganz hat fertig werden können. Den noch ausstehenden Beweis für diese Form und die folgenden hat erst LAGRANGE gegeben. Siehe die Anmerkung p. 194.

1) Hierfür ist der Brief EULERS an GOLDBACH vom 28. August 1742, *Corresp. math. et phys.* I, p. 144, von ganz besonderem Interesse. In diesem Briefe gibt EULER bereits den Hauptinhalt der Abhandlung 164 und zwar mit prophetischen Worten.

lung 158 gerade noch gestreift. Sie hatte ihn, wie wir gesehen haben, zur Entwickelung des Produktes $(1-x)(1-x^2)(1-x^3)\cdots$ veranlaßt, die zu jener ϑ-Reihe geführt hatte. Die Entwickelung des reziproken Produktes enthält in ihren Koeffizienten die Lösung der gestellten Aufgabe. Mehr bietet auch die *Introductio* nicht zu dieser Frage. In der vorliegenden Abhandlung aber entwickelt EULER eine Reihe wichtiger Formeln für $n^{(\infty)}$, unter denen die Gleichung

$$n^{(\infty)} = (n-1)^{(\infty)} + (n-2)^{(\infty)} - (n-5)^{(\infty)} - (n-7)^{(\infty)} + (n-12)^{(\infty)} + (n-15)^{(\infty)} - \cdots$$

wegen ihrer Verwandtschaft mit der ϑ-Reihe besonders zu erwähnen ist. Außerdem zeigt er, wie man mit Benutzung der schon berechneten Zahlen $n^{(m)}$, z. B. mit Benutzung von $n^{(20)}$, zu einer stark abgekürzten Berechnung der Zahlen $n^{(\infty)}$ gelangen kann.

Wie in der *Introductio* schließt sich daran die weitere Aufgabe, anzugeben, wie oft sich eine Zahl in ungleiche Teile zerlegen lasse, und es wird gezeigt, daß dies ebenso oft möglich ist, als sich dieselbe Zahl aus nur ungeraden Zahlen, seien es gleiche oder ungleiche, zusammensetzen läßt. Diese Aufgabe leitet daher zu solchen über, bei denen von den Summanden gewisse Qualitäten verlangt werden, z. B. der geometrischen Reihe 1, 2, 4, 8, 16, 32 etc. anzugehören, wobei wiederum Gleichheit der Summanden ausgeschlossen oder auch zugelassen werden kann.

Den Schluß der Abhandlung bildet endlich eine große Tabelle für die Zahlen $n^{(m)}$, die für $n=1, \ldots 59$ und für $m=1, \ldots 20$ und $m=\infty$ zusammengestellt ist und die zugleich auch ihre Entstehungsweise erkennen läßt. Die entsprechende Tabelle der *Introductio*, die nur die fertigen Zahlen bietet, reicht zwar bis $n=69$, aber dafür auch nur bis $m=11$, ohne die Reihe $m=\infty$ zu enthalten.

Mit der Abhandlung 164, die aus dem Jahre 1747 stammt, aber erst 1751 veröffentlicht wurde und zwar im letzten Bande der alten Commentarii, kehren wir wieder zu einem früheren Thema zurück, das mit der Theorie der quadratischen Reste zusammenhängt. Ihrem Hauptinhalte nach besteht diese Abhandlung aus 59 Sätzen, die ohne Beweis mitgeteilt werden und die sich auf die Divisoren der Zahlen von der Form pa^2+qb^2 beziehen.[1]) Wie EULER später selbst in der Abhandlung 598 sagt, hatte er diese Sätze größten-

1) Es ist schon früher (siehe die Anmerkung p. VII) darauf aufmerksam gemacht worden, daß die aus demselben Jahre 1747 stammende Abhandlung 134 im ersten Bande der neuen Commentarii erschienen ist. Dieser Umstand und die Ähnlichkeit der Titel beider Abhandlungen hat gelegentlich zu Mißverständnissen geführt (siehe die Bemerkungen von G. ENESTRÖM, Biblioth. Mathem. 12_3, 1911/2, p. 266). Zwischen den beiden Abhandlungen 134 und 164 bestehen aber nur wenige Beziehungen, denn von sämtlichen in 164 auftretenden Formen wird in 134 nur die erste, nämlich a^2+b^2, behandelt. Von den andern Formen hat EULER selbst überhaupt nur noch die Form a^2+3b^2 erledigt, aber erst in der Abhandlung 272, während er mit der Form a^2+2b^2,

teils nur durch Induktion gefunden. Um so wichtiger sind daher die hinzugefügten Anmerkungen, die freilich auch nicht überall als beweiskräftig gelten sollen. Dazu gehört namentlich, daß alle Divisoren von a^2+qb^2, abgesehen von 2 und q, in der Form $4qm+\alpha$ enthalten seien und daß sich diese Form für $q=4n-1$ auf $2qm+\alpha$ reduziere; ferner daß pa^2+qb^2 keinen Divisor habe, der nicht zugleich Divisor von a^2+pqb^2 ist, etc. Gegenstand besonderer Untersuchung ist dann die Frage, welche Werte für α zulässig seien, damit $4Nm+\alpha$ Teiler von a^2+Nb^2 sei: α muß quadratischer Rest von $4N$ sein; sind x und y Werte von α, so gilt dies auch für xy und allgemein für $x^\mu y^\nu$ etc., alles Sätze, die EULER erst viel später (in der Abhandlung 242) systematisch behandelt und bewiesen hat.

Die trotz mangelnder Beweise so inhaltsreiche Abhandlung ist ein merkwürdiges Beispiel für die außerordentliche Divinationsgabe EULERS.[1]) Ganz besonders aber zeigt sich das gegen den Schluß der Abhandlung. Denn bei den entsprechenden Untersuchungen der Divisoren von a^2-Nb^2, insbesonders bei der Beantwortung der Frage, welche Werte jetzt für α geeignet seien, damit $4Nm\pm\alpha$ Divisor sei, stellt sich — dem Autor freilich noch unbewußt — das Reziprozitätsgesetz der quadratischen Reste ein, das EULER mit aller Bestimmtheit erst in der Abhandlung 552 ausgesprochen hat. KRONECKER war der erste, der dies bemerkt hatte. Ich habe seine Erklärungen im Wortlaut (siehe die Anmerkung p. 217) mitgeteilt und glaube, nichts weiter hinzufügen zu sollen.

Noch sei hingewiesen auf die vielen interessanten Folgerungen, die EULER an seine Mitteilungen anknüpft und die sich auf Ausdrücke beziehen, die niemals Quadrate sein können. Als Beispiel mag die Formel $4mn-m-n$ gelten, mit der sich EULER schon früh beschäftigt hat (siehe die Anmerkung p. 360).

Die Abhandlung 167, die 1748 zugleich mit der Abhandlung 134 der Petersburger Akademie vorgelegt wurde, gehört zu denen, die zahlentheoretische Untersuchungen in geometrischem Gewande enthalten. Einkleidungen dieser Art waren schon bei DIOPHANT sehr beliebt. Das ganze sechste Buch seiner *Arithmetik* ist mit zahlentheoretischen Aufgaben gefüllt, die sich auf das rechtwinklige Dreieck beziehen, und so spielen derartige Untersuchungen denn auch in den FERMATSCHEN Randbemerkungen eine große Rolle. Ein Beispiel dafür hat uns schon die Abhandlung von FRÉNICLE geboten und auch die vorliegende Abhandlung EULERS verdankt ihre Entstehung einer solchen Randbemerkung. Es sei gleich

---

wie er in der Abhandlung 256 offen zugibt, nicht ganz hat fertig werden können. Den noch ausstehenden Beweis für diese Form und die folgenden hat erst LAGRANGE gegeben. Siehe die Anmerkung p. 194.

1) Hierfür ist der Brief EULERS an GOLDBACH vom 28. August 1742, *Corresp. math. et phys.* I, p. 144, von ganz besonderem Interesse. In diesem Briefe gibt EULER bereits den Hauptinhalt der Abhandlung 164 und zwar mit prophetischen Worten.

hier bemerkt, daß EULER außer dieser Abhandlung 167 noch sechs andere verfaßt hat, in denen DIOPHANTISCHE Probleme in geometrischem Gewande auftreten. Es sind die Abhandlungen 451, 713, 732, 748, 754, 799. Von ihnen hatte einst JACOBI[1]) an FUSS geschrieben: „Aber ich beschwöre Sie, wenn es nicht schon geschehen ist, die Abh. 321—27, welche sich unglücklicher Weise unter Geometrie verirrt haben, mit aufzunehmen, welche durchaus zu den DIOPHANTISCHEN Problemen gehören. Denn diese zusammen zu haben, ist eine wesentliche Annehmlichkeit".

In der Abhandlung 167 handelt es sich darum, ein rechtwinkliges Dreieck in rationalen Zahlen ausgedrückt zu finden, so daß jede der beiden Katheten um den Flächeninhalt vermindert eine Quadratzahl liefere.[2]) FERMAT hatte diese Aufgabe gestellt im Anschluß an eine ähnliche bei DIOPHANT und sie als sehr schwierig bezeichnet. EULER gibt zunächst drei Sonderlösungen, die er durch Zahlenbeispiele illustriert, um dann zur Solutio generalis überzugehen. Diese beruht wesentlich auf den Eigenschaften der Zahlen, die in der Form $2t^2 - u^2$ oder $t^2 - 2u^2$ enthalten sind. Zu diesen Zahlen gehören zunächst alle Quadratzahlen, ferner nach Abhandlung 164 die Primzahlen 2 und $8m \pm 1$ und schließlich die Produkte, die sich aus allen genannten bilden lassen. Denn so wie die Divisoren der Zahlen $2t^2 - u^2$ wieder von derselben Form sind, so ist auch das Produkt zweier Zahlen dieser Art wieder von derselben Art. Auf Grund dieser Sätze stellt EULER für die in seiner Solutio generalis auftretenden Zahlen eine Tabelle auf, die sich beliebig weit fortsetzen läßt und die ihm beliebig viele Dreiecke liefert, wie sie das Problem verlangt.

Wir kommen jetzt zu den Abhandlungen 175, 243 und 244, von denen schon früher die Rede war, indem sie wie die Abhandlungen 100 und 152 der Theorie der Divisorensummen gewidmet sind. Die französisch geschriebene Abhandlung 175, die aus dem Jahre 1747 stammt, ist 1751 in der wenig bekannten Bibliothèque impartiale erschienen. Dieser Umstand erklärt, daß sie sowohl JACOBI als auch FUSS unbekannt geblieben ist. Denn das Manuskript, von dem JACOBI in seinem großen Briefe an FUSS vom März/April 1848[3]) spricht, stimmt zwar im wesentlichen mit der Abhandlung 175 überein, zeigt aber doch so viele Abweichungen, daß es unmöglich als Druckvorlage zu dieser gedient haben kann. Es

1) Siehe P. STÄCKEL und W. AHRENS, *Der Briefwechsel* etc., p. 24. Die sechs Abhandlungen 321—27 (324 ist nämlich mit 321 identisch) der FUSSSCHEN Liste der Schriften EULERS vom Jahre 1843 sind die Abhandlungen 451, 713, 167, 732, 748, 754 des ENESTRÖMSCHEN Verzeichnisses. Sie sind, ebenso wie die Abhandlung 799 (= Da 6 bei FUSS), alle in die *Comment. arithm.* aufgenommen und auch in unserer Ausgabe den arithmetischen Abhandlungen zugeteilt worden.

2) Zu den Abhandlungen EULERS, die sich auf DIOPHANTISCHE Probleme beziehen, ist mit Vorteil das p. 404 erwähnte Werk von T. L. HEATH, *Diophantus of Alexandria*, zu benutzen, insbesonders Section VI des Supplements: Some solutions by EULER.

3) Siehe P. STÄCKEL und W. AHRENS, *Der Briefwechsel* etc., p. 59.

ist denn auch 1849 in den *Comment. arithm.* und 1862 in den *Opera postuma* als „ineditum" abgedruckt[1]) worden, ohne daß die Herausgeber von der früheren Publikation in der Bibliothèque impartiale Kenntnis gehabt hätten.

Die Abhandlung 175 wird eröffnet mit einigen grundlegenden Sätzen über die Divisorensummen $\int n$, Sätzen, die sich im wesentlichen schon bei SCHOOTEN und WALLIS finden. Daran schließt sich eine Tabelle für die Divisorensummen der Zahlen $n = 1, \dots 100$, die namentlich illustrieren soll, wie diese Summen eine scheinbar ganz gesetzlos verlaufende Zahlenreihe darstellen. Und dann kommt als Überraschung die berühmte Rekursionsformel

$$\int n = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \int(n-15) \\ - \int(n-22) - \int(n-26) + \text{etc.}$$

Zu dieser Formel, die durch eine große Anzahl von Beispielen verifiziert wird, war EULER geführt worden, als er bei seinen Untersuchungen über die *Partitio numerorum* in den Abhandlungen 158 und 191 das Produkt

$$(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)\cdots$$

in die Reihe

$$1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \cdots$$

entwickelt hatte. Die Gleichheit der beiden unendlichen Ausdrücke, des Produktes und der Reihe, hatte freilich EULER, wie er selbst sagt, nicht durch einen Beweis, sondern nur durch Induktion, wenn auch durch eine weit ausgedehnte, festgestellt. Unter der Voraussetzung aber, daß diese Gleichheit bewiesen sei, leitet er aus den beiden Ausdrücken durch logarithmische und gewöhnliche Differentiation zwei neue Formeln her, aus deren Vergleichung sofort die Rekursionsformel hervorgeht. Abermals also sind es hier wie in den Abhandlungen 158 und 191 die Hülfsmittel der höheren Analysis, die zu wichtigen zahlentheoretischen Ergebnissen geführt haben.

Die nach ENESTRÖM wahrscheinlich 1751 verfaßte Abhandlung 243 *Observatio de summis divisorum*, der ein sehr ausführliches Summarium vorausgeht, ist nur eine neue Redaktion der Abhandlung 175. Sie wurde von EULER am 6. April 1752 der Petersburger Akademie vorgelegt, während jene schon am 22. Juni 1747 in der Berliner Akademie gelesen worden war.[2]) Beide Redaktionen stimmen bis auf einige Kleinigkeiten vollständig miteinander überein, indessen ist die lateinische doch keine Übersetzung der französischen.[3])

1) Wenn in dem ENESTRÖMSCHEN *Verzeichnis* (p. 43) diese Abdrucke mit 175a und 175b bezeichnet werden, so ist dagegen nicht viel zu sagen. Aber der Ausdruck „Wieder abgedruckt" sollte nicht auf die Abhandlung 175 bezogen werden.

2) Ihren Hauptinhalt hatte EULER am 1. April 1747 GOLDBACH mitgeteilt, *Corresp. math. et phys.* I., p. 407.

3) Sie ist auch keine Übersetzung der Redaktionen 175a und 175b. Siehe Anmerkung 1.

Die folgende kurze, aber inhaltsschwere Abhandlung 244, deren Exhibitionsdatum unbekannt ist und die ENESTRÖM daher in seinem *Verzeichnis* (zweite Abt.) unter dem Druckjahre 1760 aufgeführt hat, — sie ist aber jedenfalls viel früheren Datums, da EULER ihren Hauptinhalt schon 1750 GOLDBACH mitgeteilt hatte (siehe die Anmerkung p. 390), — bringt die Untersuchungen von 175 und 243 zum Abschluß, indem jetzt EULER den noch ausstehenden Beweis für die Entwickelung des Produktes $(1-x)(1-x^2)(1-x^3)\cdots$ liefert. „Ein Meisterstück" sagt JACOBI bei der Erwähnung[1]) dieser Abhandlung. Um ihr einen selbständigen Charakter zu verleihen, wiederholt EULER zum Schlusse auch noch den früheren Beweis für seine Rekursionsformel, der nun nicht mehr auf Induktion, sondern auf gesicherter Basis ruht.

Schon bei verschiedenen Gelegenheiten, so namentlich in den Abhandlungen 134 und 164, hatte sich EULER mit den Eigenschaften der Zahlen von der Form a^2+b^2 zu beschäftigen gehabt. Einer systematischen Untersuchung dieser Aggregate ist die Abhandlung 228 gewidmet, die 1758 veröffentlicht wurde. Nach ENESTRÖMS Verzeichnis stammt sie wahrscheinlich aus dem Jahre 1749 und wurde nach einer Notiz auf der ersten Seite des Manuskriptes am 29. März 1751 der Petersburger Akademie vorgelegt; das Wesentlichste daraus hatte EULER aber schon am 6. Mai 1747 GOLDBACH brieflich mitgeteilt.[2]) Nach einigen Vorbereitungen beweist EULER zunächst, daß das Produkt zweier Zahlen von der Form a^2+b^2 wieder als Summe von zwei Quadraten darstellbar ist, und zwar auf doppelte Art.[3]) Er beeilt sich aber hinzuzufügen, daß daraus noch nicht ohne weiteres geschlossen werden dürfe, es müsse nun auch umgekehrt, wenn ein Produkt pq und der eine Faktor p von der Form a^2+b^2 seien, der andere Faktor q gleichfalls diese Form haben. Die drastische Art, wie EULER diesen Schluß zurückweist, entbehrt nicht eines gewissen Humors und das anmutige Beispiel mit den geraden Zahlen kehrt denn auch des öfteren wieder.[4]) Zunächst aber beweist EULER, daß diese Umkehrung des Produktensatzes richtig ist, falls p eine Primzahl bedeutet. Ist aber pq die Summe zweier Quadrate, während q nicht von dieser Form ist, so ist auch p, falls Primzahl, nicht von dieser Form, oder hat, falls zusammengesetzt, wenigstens einen Primfaktor,

1) Siehe P. STÄCKEL und W. AHRENS, *Der Briefwechsel* etc., p. 63.

2) Siehe die Anmerkung p. 295.

3) Dieser Satz wird gewöhnlich LEONARDO PISANO zugeschrieben und er findet sich auch in der Tat in seinem *Liber quadratorum* (*Scritti di* LEONARDO PISANO pubbl. da B. BONCOMPAGNI, vol. II, Roma 1862, p. 257). Es kann aber keinem Zweifel unterliegen, daß der Satz schon DIOPHANT bekannt war (siehe die Anmerkung p. 301). Der Einwand, daß er bei diesem nur in einem Zahlenbeispiel auftrete und nicht allgemein ausgesprochen werde, ist nicht stichhaltig, da DIOPHANT die Gewohnheit hatte, seine Untersuchungen an bestimmte Zahlenbeispiele anzuknüpfen, und man ihm dann überhaupt die Kenntnis allgemeiner Sätze absprechen müßte.

4) Siehe z. B. § 19 der Abhandlung 272 (p. 566).

der nicht von dieser Form ist. Ist ferner die Summe zweier Quadrate, die unter sich prim sind, durch eine Zahl p teilbar, so läßt sich stets eine andere Summe $c^2 + d^2 < \frac{1}{2}p^2$ angeben, die auch durch p teilbar ist. Mit Hülfe dieser Sätze gelangt EULER zu dem wichtigen Resultate, daß die Summe zweier Quadratzahlen, die unter sich prim sind, keinen Divisor zuläßt, der nicht selbst Summe zweier Quadrate ist. Die Beweisführung gründet sich auf die Methode der unbegrenzten Abnahme, von der schon p. XV die Rede war.

Obwohl nun EULER in der Abhandlung 134 bewiesen hatte, daß die Summe zweier Quadrate, die unter sich prim sind, außer der Zahl 2 nur Primfaktoren der Form $4n+1$ zuläßt, so war damit doch noch nicht bewiesen, daß auch umgekehrt jede Primzahl der Form $4n+1$ Teiler einer solcher Quadratsumme sein müsse. Freilich — sollte es möglich sein, das zu beweisen, so war nach dem zuletzt gewonnenen wichtigen Resultate auch der berühmte, von FERMAT ohne Beweis ausgesprochene Satz gesichert, daß jede Primzahl $4n+1$ selber Summe zweier Quadrate sei. Diese Lücke auszufüllen wollte aber EULER damals trotz einem energischen Anlaufe noch nicht gelingen. Immerhin kam er bei seinem *Tentamen demonstrationis* dem Ziele sehr nahe. Denn da nach FERMAT für je zwei Zahlen a und b, die nicht selbst durch $p = 4n+1$ teilbar sind, $a^{4n} - b^{4n} = (a^{2n} - b^{2n})(a^{2n} + b^{2n})$ durch p teilbar sein muß, so genügt es, zwei solche Zahlen zu ermitteln, für die $a^{2n} - b^{2n}$ durch p nicht teilbar ist. Für diese muß dann $a^{2n} + b^{2n}$ durch p teilbar sein und dann folgt, daß p als Teiler einer Quadratsumme selber eine Quadratsumme ist. EULER war zwar überzeugt, daß es für jede Primzahl $4n+1$ solche Zahlen a und b geben müsse, er erklärt aber offen, einen strengen Beweis dafür nicht leisten zu können.

So wendet er sich denn am Schlusse der Abhandlung 228 zu Fragen mehr praktischer Art und beweist die beiden Sätze: Wenn sich eine Zahl $4n+1$ nur auf eine einzige Art als Summe von zwei Quadraten, die unter sich prim sind, darstellen läßt, dann ist sie sicher eine Primzahl; wenn sich aber eine Zahl auf zwei verschiedene Arten in zwei Quadrate auflösen läßt, dann ist sie sicher zusammengesetzt. Hieran schließen sich einige durch ihre zweckmäßige Anordnung ausgezeichnete und durch Beispiele illustrierte Rechnungsvorschriften zur Prüfung, ob eine Zahl von der Form $4n+1$ prim sei oder nicht. Mit Recht hebt EULER hervor, welch große Erleichterung sein Verfahren gegenüber dem auf ERATOSTHENES zurückgehenden Divisionsverfahren darbietet. In der Tat erfordert seine Methode nach einer einzigen Subtraktion nur Additionen einfachster Art.

Als die Abhandlung 228 im Jahre 1758 im Druck erschien, war EULER schon seit neun Jahren im Besitze des noch fehlenden Beweises.[1]) Die Abhandlung 241, die ihn enthält,

1) Siehe die Anmerkung 1 p. 328. Hieraus und aus der Anmerkung p. 295 dürfte hervorgehen, daß die Abhandlung 228 schon vor 1749 und ebenso die Abhandlung 241 vor 1750 verfaßt worden ist.

wurde aber erst 1760 veröffentlicht. Der Beweis ist sehr einfach. Um zu zeigen, daß nicht alle Zahlen $a^{2n}-b^{2n}$ durch $4n+1$ teilbar seien, geht EULER von der Reihe

$$1,\ 2^{2n},\ 3^{2n},\ 4^{2n}, \ldots (4n)^{2n}$$

aus und bildet die Differenzen

$$2^{2n}-1^{2n},\ 3^{2n}-2^{2n},\ 4^{2n}-3^{2n}, \ldots (4n)^{2n}-(4n-1)^{2n}.$$

Wären nun alle diese durch $4n+1$ teilbar, so müßten auch ihre Differenzen, d. h. die zweiten Differenzen der gegebenen Reihe, durch $4n+1$ teilbar sein, dann aber auch die dritten, vierten etc. Die Differenzen der Ordnung $2n$ aber sind alle gleich $1\cdot 2\cdot 3 \cdots 2n$ und also durch die Primzahl $4n+1$ nicht teilbar.

Der Beweis, durch den es EULER endlich gelungen war, den berühmten FERMATSCHEN Satz zu sichern, daß sich jede Primzahl $4n+1$ als Summe zweier Quadrate darstellen lasse oder daß, wie man auch sagen kann, die Zahl -1 quadratischer Rest aller Primzahlen $4n+1$ sei, ist noch in anderer Hinsicht bemerkenswert. Denn mit diesem Beweise hat EULER der Zahlentheorie ein neues allgemeines Beweismittel zugeführt, nämlich die Methode der Differenzen, ein Beweismittel, das sich in der Hand des Meisters als ein ebenso nützliches Instrument erweisen sollte wie FERMATS Methode der unbegrenzten Abnahme. Weitere Belege dafür bieten die Abhandlungen 262 (§ 72) und 272 (§ 38) dieses Bandes.

An den Beweis, daß sich jede Primzahl $4n+1$ als Summe zweier Quadrate darstellen läßt, schließt sich nun auf Seite 13 desselben Bandes der Novi Commentarii eine neue Abhandlung an, aber ohne besonderen Titel. Wäre nicht eine neue Paragrapheneinteilung da, so müßte man, ohne das Summarium gelesen zu haben, zunächst glauben, daß es sich nur um eine Fortsetzung handle. Der Titel dieser neuen Abhandlung 242 ist von JACOBI vorgeschlagen worden und zwar auf Grund des Titels einer Abhandlung, die EULER am 17. Juni 1751 in der Berliner Akademie gelesen hatte. Da dieser Titel auch in das ENESTRÖMSCHE Verzeichnis übergegangen ist, so soll er jetzt bleiben. Besser aber wäre wohl die Überschrift *Fundamenta theoriae residuorum quadraticorum* gewesen, denn der weitaus größte und wichtigste Teil der Abhandlung ist diesen Grundlagen gewidmet und die Darstellbarkeit der Zahlen durch vier Quadrate erscheint nur zum Schluß als Anwendung. Damit ist denn auch schon der Hauptinhalt der Abhandlung charakterisiert. Mit ihr erst beginnt die eigentliche Theorie der quadratischen Reste, wenn auch in den Abhandlungen 134 und 164 schon wichtige Resultate vorausgenommen worden waren. Durch sie werden die Ausdrücke *Rest* und *Nichtrest* als bleibende termini technici in die Zahlentheorie eingeführt. Für jede Zahl p ist die Anzahl der Nichtreste wenigstens $\frac{p-1}{2}$ oder $\frac{p-2}{2}$, je nachdem p ungerade oder gerade ist. Ist r ein Rest, so sind auch alle Potenzen von r Reste. Daher muß es einen Exponenten $\lambda < \frac{p}{2}$ geben, sodaß r^{λ} durch p dividiert den Rest 1 zurückläßt. Das Produkt aus zwei Resten ist ein Rest. Dabei arbeitet EULER beständig mit dem Begriffe der Kongruenz in

bezug auf den Modul p, ohne freilich dafür eine besondere Terminologie einzuführen. Unter Beschränkung auf ungerade Primzahlen $p = 2q + 1$ wird dann weiter bewiesen, daß es genau q Reste und q Nichtreste gibt, ferner daß das Produkt aus einem Rest und einem Nichtrest ein Nichtrest, das Produkt aus zwei Nichtresten aber ein Rest ist. Die folgenden Untersuchungen stützen sich auf den Begriff des *Komplementes* eines Restes r, worunter EULER die Zahl $p - r$ oder $-r$ versteht. Kommt unter den Resten das Komplement auch nur eines einzigen Restes vor, so kommen die Komplemente aller vor. Die Anzahl q der Reste muß dann gerade sein, also p die Form $4n+1$ haben. Ist dagegen p von der Form $4n-1$, so kann sich unter den Resten auch nicht das Komplement eines einzigen befinden. Daraus ergibt sich z. B. leicht, daß $4mn - m - n$ niemals ein Quadrat sein kann, ein Satz, der bei EULER oft wiederkehrt (siehe p. XXI).

An den Unterschied zwischen den Primzahlen $4n + 1$ und $4n - 1$ schließt EULER sodann weitere Anwendungen auf die Summen von zwei und drei Quadraten an, um sich dann endlich zum Beweise des Satzes zu wenden, daß sich jede Zahl als Summe von vier oder weniger Quadraten darstellen lasse.[1]) Dieser Satz, der für die ganze Abhandlung den Titel abgegeben hat, war vor FERMAT schon von BACHET ausgesprochen worden (siehe die Anmerkung 4 p. 358). Ganz ans Ziel kommt EULER freilich nicht, wie er auch selbst zugibt, aber bei seinem Versuche, den Satz zu beweisen, gelangt er zu der berühmten Identität, nach der das Produkt zweier Summen von vier Quadraten wieder eine Summe von vier Quadraten ist. Schließlich beweist er, daß der Satz von BACHET richtig ist, wenn Brüche nicht ausgeschlossen werden. Daß der Satz auch in ganzen Zahlen gilt, hat zuerst LAGRANGE bewiesen, was dann EULER veranlaßt hat, sofort auch seinerseits einen Beweis zu geben, der die frühere Bedingung nicht mehr enthält.[2])

Die Abhandlung 253 vom Jahre 1753, zu der wir nun gelangen, gehört wieder vollständig dem Ideenkreise DIOPHANTS an. Sie handelt von Aufgaben, die scheinbar mehr als bestimmt sind, insofern als die Zahl der Bedingungen die Zahl der verfügbaren Größen übersteigt, und die doch noch unendlich viele Lösungen zulassen. Freilich müssen diese Bedingungen mit einer gewissen Kunst gestellt werden. Welche Rolle bei derartigen Aufgaben die *Porismen* DIOPHANTS, „in quibus tota solutionis vis continetur", gespielt haben und von welcher Art diese Porismen überhaupt gewesen sind, ist aus den spärlichen Überlieferungen (in DIOPHANTS *Arithmetik* kommen nur drei darauf bezügliche Zitate vor) schwer zu entscheiden. EULER selbst bezeichnet als das Wesen der Sache, „daß, wenn gewissen Bedingungen auf eine gewisse Weise Genüge geleistet werde, dann zugleich auch andere

1) Um diesen Satz hatte sich EULER schon seit 1730 bemüht. Den freilich noch nicht ganz vollständigen Beweis teilte er am 12. April 1749 GOLDBACH mit. Siehe *Corresp. math. et phys.* I, p. 21, 28, 35, 40 etc., 493, 505.

2) Siehe die Anmerkung 2 p. 370.

Bedingungen gewissermaßen von selbst erfüllt würden, sodaß es nicht nötig sei, die Rechnung noch besonders auf diese zu erstrecken." Sind also beispielsweise P, Q, R etc. und W Funktionen von x, y, z etc., so werden alle Ausdrücke $P^2 + \alpha W$, $Q^2 + \beta W$, $R^2 + \gamma W$ etc. von selbst Quadrate sein, sobald nur für x, y, z etc. Werte gewählt werden, für die $W = 0$ ist. Mit Hülfe dieses Kunstgriffes löst EULER eine große Anzahl von Aufgaben, die ohne diesen Schlüssel unüberwindliche Schwierigkeiten bieten würden.

Zu DIOPHANT gehört auch die folgende Abhandlung 255 aus dem Jahre 1754, die sich mit der Lösung der Gleichung

$$x^3 + y^3 + z^3 = v^3$$

beschäftigt. EULER gibt zunächst einige spezielle Lösungen, von denen sich eine schon bei VIETA findet, um dann das Problem ganz allgemein zu lösen. Die Lösung beruht wesentlich auf dem Satze, daß Zahlen der Form $p^2 + 3q^2$ nur durch Zahlen derselben Form geteilt werden können, ein Satz, der erst in der Abhandlung 272 dieses Bandes bewiesen wird. Aus der allgemeinen Lösung leitet dann EULER wieder eine große Anzahl besonderer Fälle ab, wobei er sich einer vorbereiteten Tabelle der Zahlen $m^2 + 3n^2$ bedient, die von $m = 0$ bis $m = 32$ und von $n = 0$ bis $n = 18$ reicht.

Der vorliegende Band enthält noch eine Abhandlung, die sich mit DIOPHANTISCHEN Aufgaben beschäftigt, nämlich die kurze Abhandlung 270 vom Jahre 1755, über die daher gleich hier berichtet werden möge. Sie stellt sich die Aufgabe, drei Zahlen x, y, z zu finden, für die die elementaren symmetrischen Funktionen

$$x + y + z, \quad xy + yz + zx, \quad xyz$$

Quadrate sind. EULER entwickelt hierfür zunächst allgemeine Formeln, aus denen er dann besondere Fälle ableitet. Die kleinsten Lösungen, zu denen er für x, y, z kommt, sind 12- und 13-stellige Zahlen. Es ist daher im höchsten Grade überraschend, daß das der Abhandlung vorausgehende Summarium, das allerdings seine eigenen Wege wandelt, als Lösungen drei dreistellige Zahlen darbietet! Daß das Summarium von EULER selbst herrührt, geht mit großer Wahrscheinlichkeit aus dem p. 520 erwähnten Briefe EULERS an den damaligen Sekretär der Petersburger Akademie G. F. MÜLLER hervor (wer hätte auch EULER so übertrumpfen können!), aber der klaffende Unterschied bleibt trotz der Tatsache, daß Abhandlung und Summarium durch einen Zeitraum von mehr als sechs Jahren getrennt sind, immer noch sehr merkwürdig. Es hat übrigens den Anschein, als ob das Summarium, das im vorliegenden Falle viel mehr bietet als die Abhandlung selbst, bisher ganz unbekannt oder wenigstens der Unterschied zwischen Summarium und Abhandlung, auf den zwar im Summarium selbst hingewiesen wird, ganz unbeachtet geblieben sei.[1])

1) F. CAJORI z. B., dem wir die Referate über Zahlentheorie im vierten Bande von CANTORS *Vorlesungen* verdanken, hat seinen Berichten, wie ich von ihm selber weiß, nicht die Editio princeps,

Die Abhandlung 256 vom Jahre 1753, von der jetzt zu sprechen sein wird, schließt sich an die Abhandlungen 228 und 241 an, zumal vom Standpunkte der Abhandlung 164 aus. Wie jene die Aggregate a^2+b^2, so behandelt 256 die Aggregate $2a^2+b^2$. Entsprechend dem Titel *Specimen de usu observationum in Mathesi pura* berechnet EULER alle Zahlen dieser Form bis 500 unter der Voraussetzung, daß a und b teilerfremd seien, und zwar so, daß er jede der Zahlenreihen $2+b^2$, $8+b^2$, $18+b^2$, $\ldots$ $450+b^2$ einzeln bis 500 entwickelt, um daraus die wichtigsten Eigenschaften dieser Zahlen zunächst durch Induktion zu gewinnen. Erst dann folgen die Beweise. Grundlegend ist, wie bei den Zahlen a^2+b^2, daß sich auch das Produkt zweier Zahlen $2a^2+b^2$ wieder in derselben Weise darstellen läßt, und zwar auf doppelte Art. Umgekehrt ergibt sich, daß eine Zahl, die auf doppelte Art in der Form $2a^2+b^2$ darstellbar ist, nicht prim sein kann. Ist ferner $2a^2+b^2$ durch eine Primzahl derselben Form teilbar, so ist auch der Quotient von derselben Form. Unter Benutzung vereinfachter symbolischer Bezeichnungen beweist sodann EULER, daß, wenn $2a^2+b^2$ durch eine Zahl teilbar ist, die nicht diese Form hat, der Quotient weder eine Primzahl dieser Form noch das Produkt aus lauter solchen Primzahlen sein kann — alles genau wie bei den Zahlen a^2+b^2. Ist ferner $2a^2+b^2$ durch eine Zahl P teilbar, ohne daß a und b einzeln dadurch teilbar sind, so läßt sich stets eine Zahl $2c^2+d^2<\frac{3}{4}P^2$ angeben, die auch durch P teilbar ist. Daraus folgt weiter, daß, wenn eine Primzahl, die in der Form $2a^2+b^2$ nicht enthalten ist, Teiler ist von einer Zahl dieser Form, aber ohne daß a und b einzeln dadurch teilbar sind, stets eine kleinere Primzahl von denselben Eigenschaften gefunden werden kann. Hieraus aber ergibt sich wieder durch die Methode der unbegrenzten Abnahme (siehe p. XV) das Resultat, daß eine Zahl von der Form $2a^2+b^2$, wo a und b teilerfremd

sondern die *Comment. arithm.* zu Grunde gelegt und so sind ihm die Summarien überhaupt unbekannt geblieben. In dem Berichte, den A. AUBRY unter dem Titel *L'oeuvre arithmétique d'EULER*, L'Enseignement mathém. **11**, 1909, p. 329, veröffentlicht hat, ist die Abhandlung 270 gar nicht erwähnt und noch weniger das Summarium. T. L. HEATH hat in seinem mehrfach zitierten Werke *DIOPHANTUS of Alexandria*, Cambridge 1910, über die Abhandlung 270 sehr ausführlich berichtet (p. 351—354), aber das Summarium ist seiner Aufmerksamkeit entgangen. Ganz umgekehrt verhält sich ein Referat aus alter Zeit. Wie aus dem *Verzeichnis* von ENESTRÖM zu ersehen ist, haben die Acta eruditorum regelmäßig über die EULERSCHEN Arbeiten kurz nach ihrem Erscheinen referiert. Ich habe aber in diesen Berichten nichts bemerkenswertes gefunden mit Ausnahme eben der Abhandlung 270. Denn über diese berichtet der Referent sehr ausführlich — indem er das Summarium, aber auch nur dieses, ohne weitere Bemerkungen vollständig und wörtlich abdruckt (siehe Nova acta erud. 1763, p. 247). Ob er auch die Abhandlung selbst angesehen hat, geht aus dem Referate nicht hervor.

Mit der Abhandlung 270 hängen aufs engste zusammen die Abhandlungen 427 und 523 des nächsten Bandes. Obwohl aber EULER in beiden die Abhandlung 270 zitiert, spricht er mit keiner Silbe von dem dazugehörigen Summarium und der darin enthaltenen einfachen Lösung. Es ist das fast noch merkwürdiger als die Existenz dieses Summariums selbst.

sind, keinen Divisor zuläßt, der nicht selbst von dieser Form ist. Als Anwendung folgt hieraus der Satz, daß, wenn eine Zahl nur auf eine einzige Weise in der Form $2a^2 + b^2$ darstellbar ist und a und b teilerfremd sind, diese Zahl sicher prim ist.

Da die Zahlen $2a^2 + b^2$ keine anderen ungeraden Zahlen als solche von der Form $8n + 1$ oder $8n + 3$ darstellen können, so können sie außer der Zahl 2 auch keine anderen Primfaktoren als solche von der Form $8n + 1$ oder $8n + 3$ besitzen. Ob nun aber auch umgekehrt jede Primzahl der Form $8n + 1$ oder $8n + 3$ Teiler sei von einer Zahl $2a^2 + b^2$ und daher selbst eine solche Zahl, ist eine andere Frage. EULER gesteht offen, daß es ihm nicht gelungen sei, einen Beweis für diese Darstellbarkeit der Zahlen $8n + 1$ und $8n + 3$ zu finden. Den Beweis hat erst LAGRANGE[1]) gegeben.

Unter der Voraussetzung aber, der Beweis sei erbracht, wendet sich EULER, ähnlich wie in der Abhandlung 228, zu einfachen und praktisch angelegten Rechnungsvorschriften für die Prüfung, ob eine Zahl von der Form $8n + 1$ oder $8n + 3$ prim sei oder nicht. EULER war jedenfalls schon lange im Besitze dieser Methode, denn er hatte mit ihrer Hülfe schon in der Abhandlung 152, die aus dem Jahre 1747 stammt, festgestellt, daß die Zahl 198 899 eine Primzahl ist. Zum Schlusse gibt EULER noch einige Umformungen der entwickelten Kriterien durch Einführung von Trigonalzahlen.

Wie die Abhandlung 242 die Grundlagen für die Theorie der quadratischen Reste geschaffen hat, so bildet die Abhandlung 262[2]) die Grundlage für die Theorie der Potenzreste. Ihre Bedeutung beruht nicht zum wenigsten auf der Einfachheit ihrer Voraussetzungen. Es sei p eine Primzahl und a prim zu p. Dann sollen die Reste untersucht werden, die bei

---

1) In der mehrfach erwähnten Abhandlung *Recherches d'arithmétique* (siehe die Anmerkung p. 194).

2) Aus den Gründen, die ich in der Anmerkung 1 p. 347 auseinandergesetzt habe, halte ich dafür, daß EULER die Abhandlung 262, oder doch wenigstens ihren ersten Teil, vor der Abhandlung 242 verfaßt habe. Wenn EULER unter dem Satze, den er „in dissertatione superiori" bewiesen habe, den Satz von FERMAT gemeint hätte, woran man ja zunächst denken könnte, würde er sich sicherlich anders ausgedrückt haben. Der fertige FERMATSCHE Satz, der bis dahin noch in dem binomischen Satze gewurzelt hatte, paßt aber auch nicht in den vorliegenden Gedankengang, denn p. 347 handelt es sich speziell um die Reihe der Potenzen $r, r^2, r^3, \ldots$ und von dieser will EULER „in dissertatione superiori" bewiesen haben, daß es eine Potenz $r^\lambda (\lambda < p)$ gäbe, so daß r^λ den Rest 1 zurücklasse. Diese dissertatio superior kann dann aber keine andere als die Abhandlung 262 sein, deren § 15 auch genau dem entspricht, worum es sich hier handelt. Daß bei der Fülle von Abhandlungen, die EULER jahraus jahrein produzierte, eine früher verfaßte später veröffentlicht wurde, hat nichts auffälliges. Gerade hierauf bezieht sich eine Anekdote, die LAGRANGE einst POISSON erzählt hat und die von G. ENESTRÖM in der Biblioth. Mathem. 12_3, 1911/2, p. 172, mitgeteilt worden ist.

der Division der aufeinander folgenden Potenzen

$$1,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6 \text{ etc.}$$

durch die Primzahl p zurückbleiben. Das ist das Thema. Und andere Hülfsmittel, als die Formulierung dieses Themas erfordert, werden auch bei der Untersuchung nicht benutzt. Sehr rasch ergibt sich das Resultat, daß eine Potenz a^λ existieren muß, die den Rest 1 liefert, und daß $\lambda < p$ ist. Ist (abgesehen von $a^0 = 1$) a^λ die kleinste Potenz, die das leistet, so geben auch alle Zahlen der Reihe

$$1,\ a^\lambda,\ a^{2\lambda},\ a^{3\lambda},\ a^{4\lambda},\ a^{5\lambda} \text{ etc.}$$

den Rest 1 und sie sind die einzigen dieser Art. Die Zahlen

$$1,\ a,\ a^2,\ a^3, \ldots\ a^{\lambda-1}$$

aber liefern jetzt lauter verschiedene Reste. Hieraus und aus dem Umstande, daß $\lambda \overline{\gtrless} p-1$ ist, folgt dann leicht, daß für den Fall $\lambda < p-1$ sofort $\lambda \overline{\gtrless} \frac{p-1}{2}$ sein muß und für $\lambda < \frac{p-1}{2}$ sofort $\lambda \overline{\gtrless} \frac{p-1}{3}$ etc. Daraus aber ergibt sich, daß λ ein Divisor von $p-1$ sein muß, und hieraus, daß auch a^{p-1} durch p dividiert den Rest 1 zurückläßt. Damit hatte Euler nicht nur einen neuen Beweis für den Fermatschen Satz gewonnen, sondern zugleich den ersten, der auf rein zahlentheoretischen Betrachtungen und zwar auf den denkbar einfachsten beruht. Es scheint übrigens, als ob auch der Beweis, den Fermat selbst in seinem berühmten Briefe an Frénicle (siehe die Anmerkung 2 p. 34) andeutet, von ähnlicher Natur gewesen sei.

Der zweite Teil der Abhandlung 262 ist nach Inhalt und Methode von etwas anderer Art als der erste. Ähnlich wie in der Abhandlung 134 und wieder mit Hülfe des binomischen Satzes beweist Euler in den Theoremen 16—18 von neuem die Sätze 10—14 jener früheren Abhandlung. Nun aber geht er einen wesentlichen Schritt weiter, indem er auch die Umkehrung dieser Sätze hinzufügt, die er damals noch nicht hatte geben können (siehe p. XVII). Im Theorem 19 beweist er nämlich: Ist $a^m - 1$ durch die Primzahl $p = mn + 1$ teilbar, so gibt es immer Zahlen x und y von der Art, daß $ax^n - y^n$ durch dieselbe Primzahl p teilbar ist. Den Beweis dieses wichtigen Satzes führt Euler mit Hülfe der Methode der Differenzen, derselben, die es ihm in der Abhandlung 241 ermöglicht hatte, zu beweisen, daß sich jede Primzahl $4n + 1$ als Summe zweier Quadrate darstellen läßt (siehe p. XXVI). Bei dem Beweise kann überdies x willkürlich gewählt, also z. B. auch gleich 1 genommen werden.

Das Theorem 11 der Abhandlung 134 lautete: Ist $a = f^2 \pm (2m+1)\alpha$ und $2m+1$ eine Primzahl, dann ist $a^m - 1$ durch $2m+1$ teilbar. Dafür kann man auch sagen: Ist D quadratischer Rest der Primzahl $p = 2m + 1$, so ist $D^{\frac{p-1}{2}} \equiv +1 \pmod{p}$. Das Theorem 19 der Abhandlung 262 enthält für $n = 2$ (und $x = 1$) die Umkehrung davon und lautet: Ist $a^m - 1$ durch die Primzahl $p = 2m + 1$ teilbar, so gibt es stets eine Zahl y der Art, daß $a - y^2$

durch p teilbar ist. Dafür kann man auch sagen: Ist $D^{\frac{p-1}{2}} \equiv +1 \pmod{p}$, so ist D quadratischer Rest von p. Es ist daher die Kongruenz

$$D^{\frac{p-1}{2}} \equiv +1 \pmod{p}$$

die notwendige und hinreichende Bedingung dafür, daß D quadratischer Rest sei von p; sie bestimmt also, wie man sagt, den quadratischen *Charakter*[1]) von D. Ebenso bestimmt die Kongruenz

$$D^{\frac{p-1}{n}} \equiv +1 \;(\text{mod. } p = mn + 1)$$

den *Charakter* der Zahl D in der Theorie der höheren Reste.

Die aus dem Jahre 1758 stammende Abhandlung 271 bringt wiederum eine wesentliche Bereicherung der Zahlentheorie, indem sie dieser die Funktion zuführt, die seit Gauss (*Disquisitiones arithmeticae*, Art. 38) allgemein mit $\varphi(m)$ bezeichnet wird und die ausdrückt, wie viele von den Zahlen $1, 2, 3, 4, \ldots m$ prim zu m sind. Auf diese Funktion wird Euler geführt, indem er die Reste betrachtet, die bei Division der Glieder einer arithmetischen Progression durch eine gegebene Zahl entstehen. Aus einer solchen Progression, deren Differenz prim zu der gegebenen Zahl n ist, gehen als Reste alle Zahlen hervor, die kleiner sind als n. Beschränkt man die Progression auf n Glieder, so werden von diesen ebensoviel prim zu n sein, als es Zahlen gibt, die kleiner als n und prim zu n sind. Für die Anzahl dieser Zahlen — Euler nennt sie zur Abkürzung *partes primae* — entwickelt nun Euler die bekannten Formeln, zunächst für das Produkt zweier Primzahlen, dann für das Produkt zweier teilerfremder Zahlen und schließlich allgemein für die Zahl

$$N = p^{\lambda} q^{\mu} r^{\nu} s^{\xi} \ldots,$$

bei der die Anzahl n der *partes primae* — ein besonderes Zeichen wie unser $\varphi(N)$ hat er dafür noch nicht — gleich

$$p^{\lambda-1}(p-1) \cdot q^{\mu-1}(q-1) \cdot r^{\nu-1}(r-1) \cdot s^{\xi-1}(s-1) \ldots$$

gefunden wird.

Euler verbindet nun diese Resultate mit der Theorie der Potenzreste, die er in der Abhandlung 262 begründet hatte. Nur wird jetzt als Divisor nicht mehr eine Primzahl, sondern eine beliebige Zahl N gedacht. Ist x zu N prim, so ergibt sich, wie früher, daß in der

1) In den *Vorlesungen über Zahlentheorie von P. G. Lejeune-Dirichlet*, herausgegeben von R. Dedekind, findet sich noch in der dritten Auflage zu diesem Satze (p. 77) die Anmerkung: „Dies Kriterium rührt wesentlich von Euler her; man vgl. z. B. die Abhandlung *Theoremata circa residua ex divisione potestatum relicta*, Nov. Comm. Petrop. VII, p. 49; aber es ist mir nicht geglückt, in seinen zahlreichen Arbeiten über diesen Gegenstand eine Stelle aufzufinden, wo dasselbe in voller Schärfe ausgesprochen wäre." Mir scheint, daß das Kriterium durch diese beiden Stellen zusammen doch scharf genug ausgesprochen sei, und vielleicht ist mit Rücksicht gerade auf diese Stellen die Anmerkung in der vierten Auflage weggelassen worden

Reihe 1, x, x^2, x^3 etc. eine Potenz auftreten muß, die den Rest 1 zurückläßt. Und ist x^ν die kleinste Potenz, die das leistet, so muß ν entweder gleich der Anzahl n der *partes primae* von N sein oder gleich einem aliquoten Teile dieser Anzahl. So gelangt denn EULER zu der berühmten Verallgemeinerung des FERMATSCHEN Satzes, die aussagt, daß $x^n - 1$ stets durch N teilbar ist, wenn x prim zu N und n die Anzahl der *partes primae* von N ist.

Wie in den Abhandlungen 228 und 241 die Aggregate $a^2 + b^2$ und in der Abhandlung 256 die Formen $2a^2 + b^2$ untersucht worden sind, so ist die Abhandlung 272 vom Jahre 1759 den Zahlen der Form $a^2 + 3b^2$ gewidmet. Eine Haupteigenschaft dieser Zahlen war schon in der Abhandlung 255, die sich mit der Gleichung $x^3 + y^3 + z^3 = v^3$ beschäftigt hatte, verwertet worden. Dies mag EULER zu der Verwechselung geführt haben, er habe jene Eigenschaften zum Beweise der Unmöglichkeit der Gleichung $x^3 + y^3 = z^3$ benutzt, während er tatsächlich einen solchen Beweis damals noch nicht veröffentlicht hatte. [1])

Zunächst kommt EULER nochmals auf die Gleichung $x^3 + y^3 + z^3 = v^3$ zurück, um der früheren Lösung eine neue Form zu geben. Dann wendet er sich zu den Zahlen der Form $a^2 + 3b^2$. Der Gang der Untersuchung ist ähnlich dem, der bei den Zahlen $a^2 + b^2$ und $2a^2 + b^2$ eingeschlagen worden war, sodaß wir uns hier kürzer fassen können. Ähnlich wie früher und wieder mit Benutzung der Methode der unbegrenzten Abnahme (siehe p. XV) ergibt sich auch hier aus verschiedenen vorbereitenden Sätzen, daß die Zahlen $a^2 + 3b^2$, wo a und b teilerfremd sind, außer der Zahl 2 keine Primfaktoren besitzen, die nicht selbst von dieser Form sind. Da nun alle Zahlen $a^2 + 3b^2$ außer der Zahl 3 die Form $6n + 1$ haben, so entsteht die Frage, ob auch umgekehrt alle Primzahlen $6n + 1$ in der Form $a^2 + 3b^2$ enthalten seien. Den Beweis hierfür leistet EULER unter Benutzung der Äquivalenz der Formen $a^2 + 3b^2$ und $m^2 + mn + n^2$ wieder mit Hülfe der Methode der Differenzen (siehe p. XXVI).

Damit war nun auch für die Zahl -3 und infolgedessen auch für die Zahl $+3$ der Charakter als quadratischer Rest festgestellt, so wie er früher in der Abhandlung 241 für die Zahl -1 gewonnen worden war.

Bei der Herstellung dieses Bandes bin ich von meinen beiden Mitredaktoren in wirksamster Weise unterstützt worden. Ihrer stillen, selbstlosen Mitarbeit verdanke ich weit mehr, als ich hier zum Ausdruck bringen kann. Möge unserer gemeinsamen Arbeit der Erfolg

1) Er hatte zwar schon 1753 an GOLDBACH geschrieben, daß er einen Beweis für die Unmöglichkeit der Gleichung $x^3 + y^3 = z^3$ gefunden habe, aber der Beweis war nicht einwandfrei, wie er selbst am Anfang und am Ende der Abhandlung 272 hervorhebt. Den wirklichen Beweis hat EULER erst 1770 in seiner *Algebra* geleistet. Siehe die Anmerkung 1 p. 558.

beschieden sein, den wir von ihr erhoffen: EULERS nie veraltende Werke weitesten Kreisen zugänglich zu machen.

Zu aufrichtigem Danke bin ich auch Herrn ENESTRÖM verpflichtet, auf dessen Rat und Hülfe ich jeder Zeit zählen durfte. Und schließlich gebühren Dank und Anerkennung der Verlagsfirma B. G. TEUBNER, die allen Wünschen des Herausgebers stets größte Bereitwilligkeit entgegengebracht hat und für deren Leistungsfähigkeit der vorliegende Band, der unter besonders schwierigen Verhältnissen entstanden ist, beredte Worte spricht.

Zürich, den 2. August 1915.

FERDINAND RUDIO.

INDEX

Insunt in hoc volumine indicis ENESTROEMIANI commentationes
26, 29, 36, 54, 98, 100, 134, 152, 158, 164, 167, 175, 191, 228, 241, 242, 243, 244, 253, 255, 256, 262, 270, 271, 272, 279

OBSERVATIONES DE THEOREMATE QUODAM FERMATIANO ALIISQUE AD NUMEROS PRIMOS SPECTANTIBUS

Commentatio 26 indicis ENESTROEMIANI
Commentarii academiae scientiarum Petropolitanae 6 (1732/3), 1738, p. 103—107

SUMMARIUM
Ex manuscriptis academiae scientiarum Petropolitanae nunc primum editum

Percelebris erat superioris saeculi Geometra Gallus FERMATIUS in investigandis numerorum proprietatibus. Inter quaestiones vero, quae de numerorum proprietatibus formari possunt, praecipua fere est ea, qua agitur de criteriis, quibus cognosci potest, utrum numerus propositus sit primus necne, i. e., an divisibilis sit per quendam numerum an secus; nec multo minoris facienda est quaestio de inveniendo numero primo quovis dato maiori. Affirmabat autem FERMATIUS omnes omnino numeros hac formula generali $2^{2^m}+1$ contentos esse primos, cuius theorematis ope altera dictarum quaestionum solvi posset. De hoc FERMATII asserto dubitari fere non poterat, quod inter numeros ab unitate usque ad 100000 progredientes nullus datur eius formae, qui non sit numerus primus. Etenim si pro m ponatur successive 1, 2, 3 et 4, prodeunt numeri 5, 7, 257 et 65537, qui revera omnes sunt numeri primi. Notavit vero celeb. EULERUS formulam FERMATIANAM fallere nonnunquam, id quod revera evenit, cum pro n ponitur 5; tunc enim prodit numerus 4294967297, qui divisibilis est per 641. Hac autem occasione auctor 6 alia proponit theoremata ad hanc rem pertinentia, quorum quidem demonstrationes non dantur, quamvis eorum veritas tentando comprobari possit.

Notum est hanc quantitatem a^n+1 semper habere divisores, quoties n sit numerus impar vel per imparem praeter unitatem divisibilis. Namque $a^{2m+1}+1$ dividi potest per $a+1$ et $a^{p(2m+1)}+1$ per a^p+1, quicunque etiam

numerus loco a substituatur. Contra vero si n fuerit eiusmodi numerus, qui per nullum numerum imparem nisi unitatem dividi possit, id quod evenit, quando n est dignitas binarii, nullus numeri $a^n + 1$ potest assignari divisor. Quamobrem si qui sunt numeri primi huius formae $a^n + 1$, ii omnes comprehendantur necesse est in hac forma $a^{2^m} + 1$. Neque tamen ex hoc potest concludi $a^{2^m} + 1$ semper exhibere numerum primum, quicquid sit a; primo enim perspicuum est, si a sit numerus impar, istam formam divisorem habituram 2. Deinde quoque, etiamsi a denotet numerum parem, innumeri tamen dantur casus, quibus numerus compositus prodit. Ita haec saltem formula $a^2 + 1$ potest dividi per 5, quoties est $a = 5b \pm 3$, et $30^2 + 1$ potest dividi per 17 et $50^2 + 1$ per 41. Simili modo $10^4 + 1$ habet divisorem 73, $6^8 + 1$ habet divisorem 17 et $6^{128} + 1$ est divisibilis per 257. At huius formae $2^{2^m} + 1$, quantum ex tabulis numerorum primorum, quae quidem non ultra 100000 extenduntur, nullus detegitur casus, quo divisor aliquis locum habeat. Hac forte aliisque rationibus FERMATIUS adductus enunciare non dubitavit $2^{2^m} + 1$ semper esse numerum primum hocque ut eximium theorema WALLISIO aliisque Mathematicis Anglis demonstrandum proposuit. Ipse quidem fatetur se eius demonstrationem non habere, nihilo tamen minus asserit esse verissimum. Utilitatem eius autem hanc potissimum praedicat, quod eius ope facile sit numerum primum quovis dato maiorem exhibere, id quod sine huiusmodi universali theoremate foret difficillimum. Leguntur haec in WALLISII *Commercio Epistolico* tomo eius Operum secundo inserto, epistola penultima.[1]) Extant etiam in ipsius FERMATII operibus p. 115 sequentia[2]): „Cum autem numeros a binario quadratice in se ductos et unitate auctos esse semper numeros primos apud me constet et iam dudum Analystis illius theorematis veritas fuerit significata, nempe esse primos 3, 5, 17, 257, 65537 etc. in infinit., nullo negotio etc."

Veritas istius theorematis elucet, ut iam dixi, si pro m ponatur 1, 2, 3 et 4; prodeunt enim hi numeri 5, 17, 257 et 65537, qui omnes inter numeros primos in tabula reperiuntur. Sed nescio, quo fato eveniat, ut statim sequens, nempe $2^{2^5} + 1$, cesset esse numerus primus; observavi enim his diebus longe alia

---

1) I. WALLIS (1616—1703), *Opera*, t. II, Oxoniae 1693, p. 857 (Epistola XLVI D. FERMATII ad D. KENELMUM DIGBY, 1658); P. DE FERMAT (1601—1665), *Oeuvres*, publiées par les soins de MM. P. TANNERY et CH. HENRY, t. II, Paris 1894, p. 402. F. R.

2) P. DE FERMAT, *Varia opera mathematica*, Tolosae 1679, p. 115; *Oeuvres de FERMAT*, t. I, Paris 1891, p. 131, t. II, Paris 1894, p. 206. F. R.

agens posse hunc numerum dividi per 641, ut cuique tentanti statim patebit.[1]) Est enim $2^{2^5}+1=2^{32}+1=4294967297$. Ex quo intelligi potest theorema hoc etiam in aliis, qui sequuntur, casibus fallere et hanc ob rem problema de inveniendo numero primo quovis dato maiore etiam nunc non esse solutum.

Considerabo nunc etiam formulam 2^n-1, quae, quoties n non est numerus primus, habet divisores, neque tantum 2^n-1, sed etiam a^n-1. Sed si n sit numerus primus, videri posset etiam 2^n-1 semper talem exhibere; hoc tamen asseverare nemo est ausus, quantum scio, cum tam facile potuisset refelli. Namque $2^{11}-1$, i. e. 2047, divisores habet 23 et 89, et $2^{23}-1$ dividi potest per 47. Video autem Cel. WOLFIUM non solum hoc in *Elem. Matheseos*[2]) editione altera non advertisse, ubi numeros perfectos investigat atque 2047 inter primos numerat, sed etiam 511 seu 2^9-1 pro tali habet, cum tamen sit divisibilis per 2^3-1, i. e. 7. Dat autem $2^{n-1}(2^n-1)$ numerum perfectum, quoties 2^n-1 est primus; debet ergo etiam n esse numerus primus. Operae igitur pretium fore existimavi eos notare casus, quibus 2^n-1 non est numerus primus, quamvis n sit talis. Inveni autem hoc semper fieri, si sit $n=4m-1$ atque $8m-1$ fuerit numerus primus; tum enim 2^n-1 semper poterit dividi per $8m-1$. Hinc excludendi sunt casus sequentes: 11, 23, 83, 131, 179, 191, 239 etc., qui numeri pro n substituti reddunt 2^n-1 numerum compositum. Neque tamen reliqui numeri primi omnes loco n positi satisfaciunt, sed plures insuper excipiuntur; sic observavi $2^{37}-1$ dividi posse per 223, $2^{43}-1$ per 431, $2^{29}-1$ per 1103, $2^{73}-1$ per 439; omnes tamen excludere non est in potestate. Attamen asserere audeo praeter hos casus notatos omnes numeros primos minores quam 50 et forte quam 100 efficere $2^{n-1}(2^n-1)$ esse numerum perfectum sequentibus numeris pro n positis 1, 2, 3, 5, 7, 13, 17, 19, 31, 41, 47, unde 11 proveniunt numeri perfecti. Deduxi has observationes ex theoremate quodam non ineleganti, cuius quidem demonstrationem quoque non habeo, verum tamen de eius veritate sum certissimus. Theorema hoc est: *a^n-b^n semper potest dividi per $n+1$, si $n+1$ fuerit numerus primus atque a et b non possint per eum dividi;*[3]) eo autem difficiliorem puto eius demonstrationem esse, quia non est verum, nisi $n+1$ sit numerus primus. Ex

1) Vide L. EULERI Commentationem 134 (indicis ENESTROEMIANI), p. 74 (§ 32) huius voluminis. F. R.

2) CHR. WOLF, *Elementa matheseos universae*, editio nova, Halae Magdeburgicae, t. I, 1730, p. 384; numerus autem 2047 etiam in editione novissima (1742) inter primos numeratur. F. R.

3) Vide Commentationem 134 huius voluminis, theorema 4. F. R.

hoc statim sequitur $2^n - 1$ semper dividi posse per $n+1$, si fuerit $n+1$ numerus primus, seu, cum omnis primus sit impar praeter 2 hicque ob conditiones theorematis, quia est $a = 2$, non possit adhiberi, poterit $2^{2m} - 1$ semper dividi per $2m+1$, si $2m+1$ sit numerus primus. Quare etiam vel $2^m + 1$ vel $2^m - 1$ dividi poterit per $2m+1$. Deprehendi autem $2^m + 1$ posse dividi, si fuerit $m = 4p+1$ vel $4p+2$; at $2^m - 1$ habebit divisorem $2m+1$, si $m = 4p$ vel $4p-1$. Haec persecutus in multa alia incidi theoremata non minus elegantia, quae eo magis aestimanda esse puto, quod vel demonstrari prorsus nequeant vel ex eiusmodi propositionibus sequantur, quae demonstrari non possunt; primaria igitur hic adiungere visum est.

THEOREMA 1

Si fuerit n numerus primus, omnis potentia exponentis $n-1$ per n divisa vel nihil vel 1 relinquit.[1])

THEOREMA 2

Manente n numero primo omnis potentia, cuius exponens est $n^{m-1}(n-1)$, divisa per n^m vel 0 vel 1 relinquit.[2])

THEOREMA 3

Sint m, n, p, q etc. numeri primi inaequales sitque A minimus communis dividuus eorum unitate minutorum, puta ipsorum $m-1$, $n-1$, $p-1$, $q-1$ etc.; his positis dico omnem potentiam exponentis A ut a^A divisam per $mnpq$ etc. vel 0 vel 1 relinquere, nisi a dividi possit per aliquem horum numerorum m, n, p, q etc.

THEOREMA 4

Denotante $2n+1$ numerum primum poterit $3^n + 1$ dividi per $2n+1$, si sit vel $n = 6p+2$ vel $n = 6p+3$; at $3^n - 1$ dividi poterit per $2n+1$, si sit vel $n = 6p$ vel $n = 6p-1$.

---

1) Quod est celebre theorema FERMATIANUM. Vide Commentationes **54**, **134**, **262** huius voluminis. F. R.

2) Hoc theorema generalius, quod in se complectitur theorema FERMATIANUM, primum ab EULERO demonstratum est in Commentatione 271 huius voluminis. F. R.

THEOREMA 5

$3^n + 2^n$ *potest dividi per* $2n + 1$, *si sit* $n =$ *vel* $12p + 3$ *vel* $12p + 5$ *vel* $12p + 6$ *vel* $12p + 8$. *Atque* $3^n - 2^n$ *potest dividi per* $2n + 1$, *si sit* $n =$ *vel* $12p$ *vel* $12p + 2$ *vel* $12p + 9$ *vel* $12p + 11$.

THEOREMA 6

Sub iisdem conditionibus, quibus $3^n + 2^n$, *poterit etiam* $6^n + 1$ *dividi per* $2n + 1$; *atque* $6^n - 1$ *sub iisdem, quibus* $3^n - 2^n$.[1])

1) Confer haec theoremata 4—6 nec non, quod occurrit in ipsa dissertatione, theorema de divisibilitate formularum $2^m + 1$ et $2^m - 1$ cum theorematis 42, 43, 50 Commentationis 164 huius voluminis. Vide etiam theorema 11 Commentationis 134 et theorema inversum, quod in Commentatione 262 (§ 72) huius voluminis continetur. F. R.

DE SOLUTIONE PROBLEMATUM DIOPHANTEORUM[1]) PER NUMEROS INTEGROS

Commentatio 29 indicis ENESTROEMIANI
Commentarii academiae scientiarum Petropolitanae 6 (1732/3), 1738, p. 175—188

SUMMARIUM

Ex manuscriptis academiae scientiarum Petropolitanae nunc primum editum

Ut Arithmetica numerorum primum universae Matheseos est fundamentum, sic cognitio proprietatum numerorum, quae altioris sunt indaginis, praeclarum quandoque in difficilioribus calculis auxilium praestat. Hanc ob causam problemata DIOPHANTEA dicta, quibus absconditae numerorum proprietates eruuntur, magni facienda sunt; non solum propter methodorum, quibus solvuntur, elegantiam et ingeniosa earum artificia, sed etiam propter earum rerum usum per universam Mathesin.

Celeb. igitur EULERUS magno studio huic rei promovendae incumbit. Id autem in problematibus DIOPHANTEIS praecipue agitur, ut quaestionibus propositis satisfiat in numeris integris. Ea vero talium problematum ratio est, ut aequatio finalis contineat litteram unam indeterminatam cum determinatis coniunctam, cuius loco oportet numerum integrum (si id quidem possibile est) substituere talem, ut quaestioni satisfiat. Iste vero numerus satisfaciens divinatione quodammodo inveniri oportet, ex quo deinceps infiniti alii reperiri queunt, per quos problema infinitis modis solvi potest. Id ergo Auctor agit, ut regulas tradat, quarum ope cognito uno numerorum satisfacientium innumerabiles alii inde elici possint.

Ponit ergo formulam ax^2+bx+c, quae debeat esse numerus quadratus, in qua a, b et c sunt numeri integri; pro x vero quoque numerus integer substituendus est. Quodsi ergo iam cognitus sit numerus n, qui pro x substitutus integram formulam reddat quadratum, ex eo invenire docet Auctor innumeros alios numeros integros aeque satisfacientes. In fine dissertationis ostendit, quomodo harum regularum ope inveniantur numeri trigonales aliique polygonales, qui sint simul quadrati.

---

1) Editio princeps: *DIOPHANTAEORUM*; summarii manuscriptum autem habet DIOPHANTEA etc. F. R.

1. Quoties in problematis DIOPHANTEIS solvendis pervenitur ad formulam, in qua plus una indeterminata non inest, maxime requiruntur numeri integri, qui loco indeterminatae positi quaesito satisfaciant. Hoc vero quando fieri non potest, numeris fractis acquiescere oportet. Observatum autem est, si in illa formula indeterminatae maxima dimensio fuerit quadratum et ipsa formula debeat esse numerus quadratus, plerumque infinitos numeros integros problema solvere, qui inter se certa lege cohaereant et seriem quandam constituant. Sed si formula vel debeat esse cubus aliave altior potentia, vel si indeterminata plures duabus habeat dimensiones, plus effici non potest, quam ut saltem numeri fracti eruantur.

2. Ita autem huiusmodi problematum omnium ratio est comparata, ut unum numerum satisfacientem divinatione inveniri oporteat, ex quo deinceps infiniti alii reperiri queant. Neque enim ad primum detegendum regula potest tradi, cum casus possint occurrere, qui omnino nullam solutionem admittunt, cuiusmodi est $3x^2+2$, quae formula nunquam fieri potest quadratum. Quamobrem in sequentibus semper ponemus unicum tantum casum esse cognitum, quo conditioni problematis satisfiat, atque regulam dabimus, qua ex illo innumerabiles alii elici possint.

3. Proposita igitur sit haec formula

$$ax^2+bx+c,$$

quae debeat esse numerus quadratus. Sintque a, b et c numeri integri et requirantur quoque numeri integri loco x substituendi. Datus autem sit numerus n, qui loco x positus reddat formulam ax^2+bx+c quadratum. Erit ergo an^2+bn+c numerus quadratus, cuius radix sit m. Iam ad alium numerum satisfacientem ex hoc dato n inveniendum pono eum esse

$$\alpha n+\beta+\gamma\sqrt{(an^2+bn+c)}$$

huncque valorem loco x substitutum reddere ax^2+bx+c quadratum, cuius radix sit

$$\delta n+\varepsilon+\zeta\sqrt{(an^2+bn+c)}.$$

Perspicuum enim est illum numerum loco x substituendum fore rationalem ob an^2+bn+c quadratum; numeros autem integros hoc modo reperiri, si modo sit n numerus integer, mox apparebit.

4. Substituatur igitur $\alpha n + \beta + \gamma\sqrt{(an^2 + bn + c)}$ loco x in $ax^2 + bx + c$ hocque facto prodibit

$$(a\alpha^2 + a^2\gamma^2)n^2 + (2a\alpha\beta + ab\gamma^2 + b\alpha)n + a\beta^2 + ac\gamma^2 + b\beta + c$$
$$+ (2a\alpha\gamma n + 2a\beta\gamma + b\gamma)\sqrt{(an^2 + bn + c)}.$$

Sed quia huius radicem quadratam ponimus $\delta n + \varepsilon + \zeta\sqrt{(an^2 + bn + c)}$, erit hinc etiam $ax^2 + bx + c$ aequalis sequenti quantitati

$$(\delta^2 + a\zeta^2)n^2 + (2\delta\varepsilon + b\zeta^2)n + \varepsilon^2 + c\zeta^2 + (2\delta\zeta n + 2\varepsilon\zeta)\sqrt{(an^2 + bn + c)}.$$

His duabus formis inter se aequatis habebuntur sequentes aequationes

$$a\alpha^2 + a^2\gamma^2 = \delta^2 + a\zeta^2, \quad 2a\alpha\beta + ab\gamma^2 + b\alpha = 2\delta\varepsilon + b\zeta^2,$$
$$a\beta^2 + ac\gamma^2 + b\beta + c = \varepsilon^2 + c\zeta^2, \quad 2a\alpha\gamma = 2\delta\zeta, \quad 2a\beta\gamma + b\gamma = 2\varepsilon\zeta.$$

Ex quibus elicitur $\delta = \frac{a\alpha\gamma}{\zeta}$ et $\varepsilon = \frac{2a\beta\gamma + b\gamma}{2\zeta}$ et valor ipsius δ in prima aequatione substitutus dat $\alpha^2\zeta^2 + a\gamma^2\zeta^2 = a\alpha^2\gamma^2 + \zeta^4$, quae in duas resolvitur $\zeta^2 = \alpha^2$ et $\zeta^2 = a\gamma^2$. Harum autem posterior, nisi sit a quadratum, locum habere nequit. Habebimus ergo $\zeta = \alpha$ et secunda aequatio factis substitutionibus hisce similiter in has resolvetur $a\gamma^2 = \alpha^2$ et $\beta = \frac{b(\alpha - 1)}{2a}$, quarum iterum posterior tantum locum habet. His inventis tertia tandem aequatio dabit $\alpha = \sqrt{(a\gamma^2 + 1)}$; inveniri igitur debet valor pro γ, quo $a\gamma^2 + 1$ fiat quadratum.

5. Sit p iste numerus, qui loco γ substitutus reddat $a\gamma^2 + 1$ quadratum, et huius radix ponatur q, ita ut sit

$$q = \sqrt{(ap^2 + 1)};$$

erit

$$\alpha = q, \quad \gamma = p, \quad \beta = \frac{b(q-1)}{2a}, \quad \delta = ap, \quad \varepsilon = \frac{bp}{2} \quad \text{et} \quad \zeta = q.$$

Ex his colligitur sequens

THEOREMA

Si ax^2+bx+c est quadratum casu, quo $x=n$, erit quoque quadratum casu, quo

$$x = qn + \frac{bq-b}{2a} + p\sqrt{(an^2+bn+c)},$$

eiusque quadrati radix erit

$$apn + \frac{bp}{2} + q\sqrt{(an^2+bn+c)}.$$

Si ergo modo bp per 2 dividi potest, radix quadrati erit numerus integer et propterea quoque valor ipsius x erit integer seu $bq-b$ dividi poterit per $2a$.

6. Quemadmodum autem ex n valore ipsius x dato inventus est alius $qn+\frac{bq-b}{2a}+pm$ posito m loco $\sqrt{(an^2+bn+c)}$, ita hac quantitate tanquam n tractata, quo casu loco m sumi debebit $apn+\frac{bp}{2}+qm$, eruetur denuo alius valor, qui loco x substitutus quaesito satisfacit, scilicet hic

$$\begin{aligned}2ap^2n &+ bp^2 + 2pqm;\\ +n&\end{aligned}$$

quadrati vero hinc orti radix erit

$$\begin{aligned}2apqn + bpq &+ 2ap^2m\\ &+ m.\end{aligned}$$

Consideretur iam illa quantitas ut n et haec ut m; habebitur quartus valor ipsius x satisfaciens hic

$$\begin{aligned}&4ap^2qn + 2bp^2q + 4ap^3m\\ &+ qn + \frac{b(q-1)}{2a} + 3pm.\end{aligned}$$

Et radix quadrati respondentis erit

$$\begin{aligned}&4a^2p^3n + 2abp^3 + 4ap^2qm\\ &+ 3apn + \frac{3bp}{2} \qquad + qm.\end{aligned}$$

7. Valores ipsius x satisfacientes una cum radicibus quadratorum respondentium ergo ita se habebunt, ut sequitur:

	Valores ipsius x	Valores $\sqrt{(ax^2+bx+c)}$
I.	n	m
II.	$qn + pm + \frac{b(q-1)}{2a}$	$apn + qm + \frac{bp}{2}$
III.	$2q^2n + 2pqm + \frac{b(q^2-1)}{a}$ $-n$	$2apqn + 2q^2m + bpq$ $-m$
IV.	$4q^3n + 4pq^2m + \frac{b(4q^3-3q-1)}{2a}$ $-3qn - pm$	$4apq^2n + 4q^3m + 2bpq^2$ $-apn - 3qm - \frac{bp}{2}$
V.	$8q^4n + 8pq^3m + \frac{4bq^2(q^2-1)}{a}$ $-8q^2n - 4pqm$ $+n$	$8apq^3n + 8q^4m + 4bpq^3$ $-4apqn - 8q^2m - 2bpq$ $+m$
	etc.	etc.

Huius progressionis haec est lex:	Huius progressionis haec est lex:
Terminus quicunque A	E
hunc sequens B	F
$2qB - A + \frac{b(q-1)}{a}$	$2qF - E$

Hae igitur progressiones, quousque libuerit, exiguo labore continuantur.

8. Perspicitur ex his formis alternos ad minimum terminos efficere ax^2+bx+c numerum quadratum integrum atque omnia omnino quadrata fieri numeros integros, si fuerit bp numerus par. Omnes autem ipsius x valores erunt numeri integri, si $b(q-1)$ dividi poterit per $2a$; sin vero hoc non fuerit, saltem alterni ipsius x valores erunt numeri integri, nam $qq-1$, i. e. ap^2, semper dividi poterit per a, siquidem, ut ponimus, p et q sint numeri integri. Praeterea notandum est in terminis istis etiam m negative accipi posse, qua ratione numerus solutionum quandoque duplicatur.

9. Intelligitur etiam, si a sit numerus quadratus, solutionem in numeris integris exhiberi non posse, nisi forte ax^2+bx+c vel ipsum est quadratum vel numero quadrato fieri potest aequale. Hanc ob rem exclusimus supra eos casus, quibus a erat quadratum, quia hic tantum de numeris integris

problema solventibus praecepta tradere instituimus. Nam si a est quadratum, nullus numerus integer potest exhiberi, qui loco p positus efficiat ap^2+1 quadratum, praeter 0. Hoc vero casu omnes valores ipsius x manent n nullusque ergo alius nisi is, qui divinatione est inventus, eruitur.

10. Quoties autem a non est numerus quadratus, semper numerus integer potest assignari, qui loco p positus efficiat ap^2+1 quadratum[1]). Quamobrem his casibus, si unicum casum elicuerimus, quo ax^2+bx+c fit quadratum, simul quoque casus infinitos exhibere poterimus, qui ax^2+bx+c in quadratum transmutent. Proposita igitur formula ax^2+bx+c hoc erit agendum: Primo coniectura detegi debebit valor ipsius x in integris, qui reddat ax^2+bx+c quadratum. Deinde etiam quaeri debet valor ipsius p, quo ap^2+1 etiam fiat quadratum. Hisque inventis ope progressionum inventarum casus infiniti innotescent.

11. Si c est quadratum, nempe $=dd$, statim apparet casus, quo ax^2+bx+d^2 est quadratum; is enim est, si $x=0$. Ponamus ergo $n=0$ eritque $m=d$ et valores ipsius x satisfacientes constituent hanc seriem

$$0,\quad dp+\frac{b(q-1)}{2a},\quad 2dpq+\frac{b(q^2-1)}{a},\cdots A,\ B,\ 2qB-A+\frac{b(q-1)}{a}.$$

Quadratorum autem, quae hinc generantur, radices erunt

$$d,\quad dq+\frac{bp}{2},\quad d(2q^2-1)+bpq,\ \ldots\ E,\ F,\ 2qF-E.$$

Harum serierum lex ut et priorum (§ 7) perspicua est; sunt enim omnes recurrentes seu quivis terminus ex duobus praecedentibus est compositus.

12. Sit $b=0$ et $d=1$, ut habeatur haec forma ax^2+1, ad quam, ut ex praecedentibus apparet, generalis ax^2+bx+c maximam partem reducitur. Huius ergo valores ipsius x respondentes in hac serie progrediuntur

$$0,\ p,\ 2pq,\ 4pq^2-p,\ \ldots\ A,\ B,\ 2qB-A,$$

1) Hanc aequationem $ap^2+1=q^2$, quae recte FERMATIANA, non PELLIANA appellari debet, FERMATIUS a. 1657 mathematicis resolvendam proposuerat. Vide P. DE FERMAT, *Varia opera mathematica*, Tolosae 1679, p. 190; *Oeuvres de Fermat*, t. II, p. 333, 334, 433. F. R.

radices vero quadratorum productorum erunt sequentes

$$1,\ q,\ 2q^2-1,\ 4q^3-3q,\ \ldots\ E,\ F,\ 2qF-E.$$

Si ergo unicus casus p, quo ap^2+1 sit quadratum, constat, huiusmodi numeri infiniti habebuntur, qui in tractatione generalis formulae ax^2+bx+c loco p et q collocari possunt.

13. Quo autem haec methodus ad quosvis casus possit accommodari, videamus primo, quos numeros pro quolibet ipsius a valore litteris p et q tribui oporteat. Debet autem p talis esse numerus, qui ap^2+1 reddat quadratum, huiusque radix erit q. Perspicuum quidem est, si unicus pro p habeatur valor idoneus, simul quoque infinitos haberi; attamen hic unicum duntaxat eumque minimum praeter 0 adhiberi convenit. Nam reliqui sequentes, qui sunt $2pq$, $4pq^2-p$ etc., solutionum numerum non multiplicant, cum valores tantum sequentes ipsius x in § 7 praebeant. Minimus autem ipsius p valor dabit omnes numeros ipsius x satisfacientes, quod maiores non faciunt.

14. Intelligatur igitur, quodsi fuerit $a=e^2-1$, minimum ipsius p valorem fore 1 ipsiusque $q=e$, deinde si fuerit $a=e^2+1$, tum esse $p=2e$ et $q=2e^2+1$. Atque si sit $a=e^2\pm 2$, erit $p=e$ et $q=e^2\pm 1$. Huiusmodi casus infiniti alii possunt definiri, quorum ingens numerus hoc continetur theoremate: *Si sit* $a=\alpha^2e^{2b}\pm 2\alpha e^{b-1}$, *erit* $p=e$ *et* $q=\alpha e^{b+1}\pm 1$, *ubi pro* α *etiam numeri fracti accipi possunt, dummodo illi per* e^{b-1} *multiplicati in integros transmutentur*. Simili modo etiam, si sit $a=(\alpha e^b+\beta e^u)^2+2\alpha e^{b-1}+2\beta e^{u-1}$, erit $p=e$ et $q=\alpha e^{b+1}+\beta e^{u+1}+1$. Atque etiam si sit $a=\frac{1}{4}\alpha^2k^2e^{2b}\pm\alpha e^{b-1}$, erit $p=ke$ et $q=\frac{1}{2}\alpha k^2e^{b+1}\pm 1$.

15. Quoties igitur a est numerus, qui in istis formulis contineatur, statim apparet valor ipsius p et q. At si a huiusmodi fuerit numerus, qui nullo modo ad illas formulas potest reduci, peculiaris ad invenienda p et q adhibenda est methodus, qua olim iam usi sunt PELLIUS[1]) et FERMATIUS.

---

1) Vide tamen, id quod ad PELLIUM attinet, G. ENESTROEM, *Über den Ursprung der Benennung „Pellsche Gleichung"*, Biblioth. Mathem. 3_3, 1902, p. 204. F. R.

Haecque methodus est universalis et aeque succedit, quemcunque numerum denotet a. Praeterea etiam ideo hic potissimum est commendanda, quod minimum ipsius p valorem, qui hoc loco requiritur, exhibeat.

16. Methodus haec extat descripta in Operibus WALLISII[1]) et hanc ob rem eam hic fusius non expono. Operandi tamen modum in unico exemplo ostendisse iuvabit, cuius inspectio ad quaeque alia solvenda perducet. Oporteat nimirum determinari minimum ipsius p valorem, quo $31p^2+1$ fit quadratum. Ad hoc efficiendum sequens instituitur calculus:

$$\sqrt{(31p^2+1)}=q, \quad \text{ergo } q>5p; \quad \text{ponatur itaque } q=5p+a;$$

$$\begin{array}{lll}
6p^2+1=10ap+a^2, & p=\dfrac{5a+\sqrt{(31a^2-6)}}{6}, & p=a+b; \\
5a^2=2ab+6b^2+1, & a=\dfrac{b+\sqrt{(31b^2+5)}}{5}, & a=b+c; \\
3b^2=8bc+5c^2-1, & b=\dfrac{4c+\sqrt{(31c^2-3)}}{3}, & b=3c+d; \\
2c^2=10cd+3d^2+1, & c=\dfrac{5d+\sqrt{(31d^2+2)}}{2}, & c=5d+e; \\
3d^2=10de+2e^2-1, & d=\dfrac{5e+\sqrt{(31e^2-3)}}{3}, & d=3e+f; \\
5e^2=8ef+3f^2+1, & e=\dfrac{4f+\sqrt{(31f^2+5)}}{5}, & e=2f+g; \\
f^2=12fg-5g^2+1, & f=6g+\sqrt{(31g^2+1)}. &
\end{array}$$

Tamdiu scilicet hae operationes continuantur, quoad in media columna perveniatur ad $\sqrt{(31g^2+1)}$ eiusdem formae, quam habuit proposita $\sqrt{(31p^2+1)}$. Perspicuum iam est, si ponatur $g=0$, fore $f=1$. Hincque retrogrediendo habebitur $e=2$, $d=7$, $c=37$, $b=118$, $a=155$, $p=273$ atque $q=1520$.

17. Quo autem non tanto opus sit labore ad valores ipsarum p et q inveniendos pro dato numero a, sequentem tabulam annexere visum est, in qua pro singulis valoribus ipsius a exhibentur minimi numeri, qui loco p substituti reddant ap^2+1 quadratum.

1) I. WALLIS, *Opera*, t. II, Oxoniae 1693, cap. 98—99, p. 418—429. Cf. quoque cap. 56—61, p. 232—250. F. R.

a	p	q	a	p	q
2	2	3	37	12	73
3	1	2	38	6	37
5	4	9	39	4	25
6	2	5	40	3	19
7	3	8	41	320	2049
8	1	3	42	2	13
10	6	19	43	531	3482
11	3	10	44	30	199
12	2	7	45	24	161
13	180	649	46	3588	24335
14	4	15	47	7	48
15	1	4	48	1	7
17	8	33	50	14	99
18	4	17	51	7	50
19	39	170	52	90	649
20	2	9	53	9100	66249 [1]
21	12	55	54	66	485
22	42	197	55	12	89
23	5	24	56	2	15
24	1	5	57	20	151
26	10	51	58	2574 [1]	19603
27	5	26	59	69	530
28	24	127	60	4	31
29	1820	9801	61	226153980	1766319049
30	2	11	62	8	63
31	273	1520	63	1	8
32	3	17	65	16	129
33	4	23	66	8	65
34	6	35	67	5967	48842
35	1	6	68	4	33

1) Hac ex tabula apparet numeros falsos $q = 66251\,(a = 53)$ et $p = 2564\,(a = 58)$, qui inveniuntur in L. EULERI *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, II, p. 328—329 (LEONHARDI EULERI *Opera omnia*, series I, vol. 1; vide ibidem editoris notam p. 386), typographico tantum errore ortos esse. F. R.

18. Hic statim occurrit modus perfacilis extrahendi quam proxime radicem quadratam ex numero quocunque non quadrato a. Quia enim est $ap^2+1=q^2$, erit $\sqrt{a}=\frac{\sqrt{(q^2-1)}}{p}$ et, si q sit numerus valde magnus, erit $\sqrt{a}=\frac{q}{p}$ quam proxime. Sed loco p possunt poni singuli termini seriei $0,\ p,\ 2pq,\ 4pq^2-p,\ \ldots\ A,\ B,\ 2qB-A$ et loco q singuli termini respondentes seriei huius $1,\ q,\ 2q^2-1,\ 4q^3-3q,\ \ldots\ E,\ F,\ 2qF-E$ (§ 12). Sit huius seriei terminus indicis $i=Q$ et illius terminus, cuius index etiam i est, $=P$; erit $\sqrt{a}=\frac{Q}{P}$. Quia vero, quo magis continuantur hae series, maiores quoque fiunt termini Q, eo propior reperietur $\sqrt{a}$ sumendis terminis serierum a primo longius distantibus. Sit exempli gratia $a=6$; erit $p=2$ et $q=5$ seriesque sibi invicem subscribantur, ut sequitur, posteriore loco superiore posita

$$\frac{1,\ 5,\ 49,\ 485,\ 4801,\ 47525,\ 470449,\ 4656965 \text{ etc.}}{0,\ 2,\ 20,\ 198,\ 1960,\ 19402,\ 192060,\ 1901198 \text{ etc.}}.$$

Sumtis igitur ultimis terminis erit $\frac{4656965}{1901198}$ ita propinquum radici quadratae ex 6, ut plus eam non excedat quam hac fractione $\frac{1}{2(1901198)^2\sqrt{6}}$. Simili modo patet radicem quadratam ex 61 fore proxime aequalem $\frac{1766319049}{226153980}$. Quae quidem radix vera aliquantulum maior est, sed excessus est minor quam $\frac{1}{2(226153980)^2\sqrt{61}}$.

19. Quaerantur omnes numeri triangulares, qui sint simul quadrati; debebit $\frac{x^2+x}{2}$ esse quadratum. Quadratum igitur quoque erit $2x^2+2x$, ex quo fit collatione cum formula ax^2+bx+d^2 (§ 11) instituta $a=2,\ b=2,\ d=0$. Sed quia est $a=2$, erit ex tabula superiore $p=2$ et $q=3$. Unde loco x substitui debebunt sequentes valores 0, 1, 8, 49, 288, 1681, 9800 etc., quo $\frac{x^2+x}{2}$ fiat quadratum. Quadratorum autem hinc ortorum radices tenebunt hanc seriem 0, 1, 6, 35, 204, 1189, 6930 etc. Vel quadrata, quorum radices continentur in hac serie, erunt numeri triangulares. Seriei quidem huius posterioris termini fiunt duplo maiores, si formentur ex serie generali $d,\ dq+\frac{bp}{2},\ d(2q^2-1)+bpq$ etc.; sed quia hi termini sunt radices ex $2x^2+2x$, debebunt dividi per 2, quo habeantur radices ex $\frac{x^2+x}{2}$.

20. Numeri polygonales l laterum exprimuntur hac formula generali $\frac{(l-2)x^2-(l-4)x}{2}$, in qua x denotat radicem numeri polygonalis. Quo ergo

huiusmodi numerus polygonalis sit quadratum, oportet $2(l-2)x^2-2(l-4)x$ esse quadratum. Statim autem unus casus apparet, quo quaesito satisfit, scilicet si $x=0$; fit enim ipsa formula $=0$. Quamobrem habebimus $n=0$ et $m=0$ et formula cum generali ax^2+bx+c comparata prodit $a=2(l-2)$ et $b=-2(l-4)$ atque $c=0$. Fiat igitur $2(l-2)p^2+1=q^2$; erunt ipsius x valores, quibus $2(l-2)x^2-2(l-4)x$ seu huius pars quarta $\frac{(l-2)x^2-(l-4)x}{2}$, i. e. ipse numerus polygonalis, fit quadratum, sequentes

$$0,\ \frac{-(l-4)}{2(l-2)}(q-1),\ \frac{-(l-4)}{l-2}(q^2-1),\ \ldots\ A,\ B,\ 2qB-A-\frac{l-4}{l-2}(q-1).$$

Qui quidem numeri omnes, si $l>4$, sunt negativi; attamen affirmativi habebuntur valores ipsius x sumto q negativo; tum enim alterni termini erunt affirmativi. Deinde etiam si inventus sit numerus negativus pro x, qui sit $-k$, poterit numerus affirmativus dari, qui eundem numerum polygonalem producat; erit nempe $x=k+\frac{l-4}{l-2}$; sed nisi sit $\frac{l-4}{l-2}$ numerus integer, hi numeri affirmativi fiunt fracti, quos hic excludimus. Hanc ob rem alternis terminis superioris seriei posito $-q$ loco q contenti esse debemus. Radices vero quadratorum $2(l-2)x^2-2(l-4)x$ his casibus resultantium tenebunt hanc progressionem, $0,\ (l-4)p,\ 2(l-4)pq,\ \ldots\ E,\ F,\ 2qF-E$.

21. Quo autem non alii numeri nisi affirmativi et integri reperiantur, alium casum, quo $2(l-2)x^2-2(l-4)x$ fit quadratum, erui oportet, qui erit, si $x=1$; prodibit enim 4. Hanc ob rem ponatur $n=1$ et $m=2$, quo facto habebuntur pro x valores sequentes

$$1,\ q+2p-\frac{l-4}{2(l-2)}(q-1),\ 2q^2-1+4pq-\frac{l-4}{l-2}(q^2-1),\ \ldots$$
$$A,\ B,\ 2qB-A-\frac{l-4}{l-2}(q-1).$$

Radices autem quadratae ex $\frac{(l-2)x^2-(l-4)x}{2}$ progredientur in hac serie

$$1,\ \frac{lp}{2}+q,\ lpq+2q^2-1,\ \ldots\ E,\ F,\ 2qF-E.$$

Quo autem omnes ipsius x valores sint numeri integri, non quidem loco q minimum valorem, sed eum, qui reddat $\frac{l-4}{2(l-2)}(q-1)$ numerum integrum, seligi convenit, id quod semper fieri poterit.

Ut si quaerantur numeri pentagonales quadrati, erit $l = 5$ et $a = 6$ atque q erit numerus ex hac serie 1, 5, 49 etc. et ipsius p valores respondentes erunt 0, 2, 20 etc. Quo igitur $\frac{l-4}{2(l-2)}(q-1) = \frac{1}{6}(q-1)$ sit numerus integer, sumi debet $q = 49$ et $p = 20$. Radices ergo numerorum pentagonalium, qui sunt quadrati, erunt

$$1, \ 81, \ 7921, \ \ldots \ A, \ B, \ 98B - A - 16,$$

qui numeri etiam in superiore serie (§ 20) continentur, si accipiatur $q = -5$; erunt enim termini alterni affirmativi. Horum autem numerorum pentagonalium radices quadratae erunt

$$1, \ 99, \ 9701, \ \ldots \ E, \ F, \ 98F - E.$$

22. Quia est $2(l-2)p^2 + 1 = q^2$, manifestum est ex praecedentibus, si fuerit $2l - 4$ quadratum, nullum numerum integrum loco p substitui posse. Hanc ob rem vel omnes numeri polygonales erunt quadrati, vel tantum nonnulli. Prius evenit, si $l = 4$; nam omnes numeri tetragonales sunt simul quadrati. Posterius vero, si sit $2l - 4 = 16$ seu 36 seu 64 etc; his enim casibus alii non erunt quadrati nisi 0 et 1. Si $2l - 4 = 16$, erit $l = 10$ ideoque numeri polygonales erunt decagonales, quorum forma est $4x^2 - 3x$. Nullusque numerus decagonalis est quadratus praeter 0 et 1 in integris.

SOLUTIO PROBLEMATIS ARITHMETICI DE INVENIENDO NUMERO QUI PER DATOS NUMEROS DIVISUS RELINQUAT DATA RESIDUA

Commentatio 36 indicis ENESTROEMIANI
Commentarii academiae scientiarum Petropolitanae 7 (1734/5), 1740, p. 46—66

1. Reperiuntur in vulgaribus arithmeticorum libris passim huiusmodi problemata, ad quae perfecte resolvenda plus studii et sollertiae requiritur, quam quidem videatur. Quamvis enim plerumque regula sit adiecta, cuius ope solutio obtineri queat, tamen ea vel est insufficiens solique casui proposito convenit, ita ut circumstantiis quaestionis parum immutatis ea nullius amplius sit usus, vel subinde etiam solet esse falsa. Ita quadratorum magicorum constructio iam pridem ab arithmeticis est tradita; quae autem cum esset insufficiens, maiora ingenia LAHIRII[1]) et SAUWERII[2]) ad perficiendum requisivit. Simili quoque modo ubique fere occurrit istud problema, ut inveniatur numerus, qui per 2, 3, 4, 5 et 6 divisus relinquat unitatem, per 7 vero dividi queat sine residuo. Methodus vero idonea ad huiusmodi problemata solvenda nusquam exhibetur; solutio enim ibi adiecta in hunc tantum casum competit atque tentando potius absolvitur.

2. Si quidem numeri, per quos quaesitus numerus dividi debet, sunt parvi, prout in hoc exemplo, tentando non difficulter quaesitus numerus in-

1) PH. DE LAHIRE (1640—1718), *Nouvelles constructions et considérations sur les quarrés magiques avec les démonstrations,* Mém. de l'acad. d. sc. de Paris 1705, p. 127. F. R.

2) J. SAUVEUR (1653—1716), *Construction générale des quarrés magiques,* Mém. de l'acad. d. sc. de Paris 1710, p. 92. F. R.

venitur; difficillima autem foret istiusmodi solutio, si divisores propositi essent valde magni. Cum itaque ad huius generis problemata solvenda methodus etiamnum habeatur nulla genuina, quae ad magnos divisores aeque pateat ac ad parvos, non inutiliter operam meam collocatam esse confido, dum in huiusmodi methodum inquisivi, qua sine tentatione pro maximis etiam divisoribus talia problemata resolvi queant.

3. Quo igitur, quae hac de re sum meditatus, distincte exponam, a casu incipio simplicissimo, quo unicus tantum datur divisor numerusque quaeritur, qui per illum divisus datum relinquat residuum. Requiratur scilicet numerus z, qui per numerum a divisus relinquat p pro residuo. Huius quidem quaestionis solutio est facillima; erit enim $z = ma + p$ denotante m numerum quemcunque integrum; interim tamen observari convenit hanc solutionem esse universalem omnesque numeros satisfacientes complecti. Praeterea ex ea quoque intelligitur, si unus habeatur numerus satisfaciens, ex eo innumerabiles alios satisfacientes quoque posse inveniri, dum ille numerus quocunque multiplo ipsius a vel augeatur vel, si fieri potest, minuatur. Erit autem p seu $0a + p$ minimus numerus satisfaciens, hunc excipit $a + p$, quem porro sequuntur $2a + p$, $3a + p$, $4a + p$ etc., qui numeri omnes constituunt progressionem arithmeticam differentiam constantem habentem a.

4. Hoc exposito sequitur casus, quo duo divisores cum suis residuis proponuntur, qui est praecipuus et sequentes omnes in se complectitur. Nam quotcunque propositi fuerint divisores, quaestio semper ad hunc casum, quo duo tantum proponuntur, reduci poterit, quemadmodum in sequentibus monstrabo. Quaeri igitur oporteat numerum z, qui per a divisus relinquat p, per b vero divisus relinquat q, sitque numerus a maior numero b. Cum ergo numerus quaesitus z ita debeat esse comparatus, ut per a divisus relinquat p, necessario in hac forma $ma + p$ continebitur eritque idcirco $z = ma + p$. Deinde ex altera conditione, qua z per b divisus relinquere debeat q, erit $z = nb + q$. Quamobrem, cum sit $ma + p = nb + q$, determinari debebunt numeri integri loco m et n substituendi, ut sit $ma + p = nb + q$; quibus inventis erit $ma + p$ seu $nb + q$ numerus quaesitus z.

5. Quia ergo est $ma + p = nb + q$, erit $n = \frac{ma + p - q}{b}$ seu posito $p - q = v$ erit $n = \frac{ma + v}{b}$. Hanc ob rem definiri oportet numerum m, ut $ma + v$ dividi

possit sine residuo per b. Quia est $a > b$, ponatur $a = \alpha b + c$; erit $n = m\alpha + \frac{mc+v}{b}$; oportet ergo, ut $mc + v$ divisionem per b admittat; sunt autem α et c numeri cogniti, qui reperiuntur ex divisione ipsius a per b; erit enim α quotus et c residuum. Ponatur porro $\frac{mc+v}{b} = A$; erit $m = \frac{Ab-v}{c}$; quare numerum A inveniri oportet, ut $Ab - v$ dividi queat per c. Si eveniat, ut v per c dividi possit, operatio iam poterit finiri; sumto enim $A = 0$ erit $m = -\frac{v}{c}$ et $z = -\frac{av}{c} + p$, quae expressio, etiamsi evadat negativa, tamen ad infinitos numeros affirmativos pro z inveniendos est idonea.

6. Sin autem v per c non potest dividi, quo $\frac{Ab-v}{c}$ fiat numerus integer, pono $b = \beta c + d$ seu divido b per c dicoque quotum $= \beta$ et residuum $= d$. Quo facto erit $\frac{Ab-v}{c} = A\beta + \frac{Ad-v}{c} = m$ debebitque $\frac{Ad-v}{c}$ esse numerus integer; sit is $= B$; fiet $A = \frac{Bc+v}{d}$. Si nunc v per d dividi poterit, facio $B = 0$ eritque $A = \frac{v}{d}$, et $m = \frac{\beta v}{d}$.

Sin autem v per d non est divisibile, pono porro $c = \gamma d + e$ eritque $A = B\gamma + \frac{Be+v}{d}$. Atque pono $\frac{Be+v}{d} = C$, ut sit $B = \frac{Cd-v}{e}$. Si nunc v per e dividi poterit, pono $C = 0$ eritque $B = -\frac{v}{e}$ et $A = -\frac{\gamma v}{e}$ atque $m = -\frac{\beta\gamma v}{e} - \frac{v}{e}$.

Sin $\frac{v}{e}$ nondum fuerit integer numerus, pono $d = \delta e + f$ eritque $B = C\delta + \frac{Cf-v}{e}$; atque facio $\frac{Cf-v}{e} = D$, ut sit $C = \frac{De+v}{f}$, ubi videndum est, utrum v per f dividi possit an secus, atque in utroque casu ut supra operatio debet institui.

7. Quia autem $a > b$ atque $b > c$ et $c > d$ etc., hac serie a, b, c, d, e, f etc. continuanda perpetuo ad minores numeros devenitur, ita ut tandem ad tam parvum perveniri oporteat, qui sit pars aliquota seu divisor ipsius v. Sunt autem c, d, e, f etc. continua residua ordinariae operationis, qua maximus communis divisor ipsorum a et b investigari solet, quam operationem hic appono:

$n = \frac{ma + v}{b}$	$b \mid a \mid \alpha$	$a = \alpha b + c$
$m = \frac{Ab - v}{c}$	$c \mid b \mid \beta$	$b = \beta c + d$
$A = \frac{Bc + v}{d}$	$d \mid c \mid \gamma$	$c = \gamma d + e$
$B = \frac{Cd - v}{e}$	$e \mid d \mid \delta$	$d = \delta e + f$
$C = \frac{De + v}{f}$	$f \mid e \mid \varepsilon$	$e = \varepsilon f + g$
$D = \frac{Ef - v}{g}$	$g \mid f \mid \zeta$	$f = \zeta g + h$
$E = \frac{Fg + v}{h}$	$h \mid g \mid \eta$	$g = \eta h + i$
$F = \frac{Gh - v}{i}$	$i \mid h \mid \theta$	$h = \theta i + k$
$G = \frac{Hi + v}{k}$	k	

8. Haec ergo operatio, qua ad maximum communem divisorem numerorum a et b uti solemus, eousque est continuanda, donec ad residuum perveniatur, quod dividat v. Quo invento sequenti modo investigabimus numerum m. Si v iam per b dividi poterit, fiet $m = 0$. Si v per c divisionem admittat, fiet $A = 0$ et $m = \frac{-v}{c}$. Si v per d dividatur, fiet $B = 0$ et $A = \frac{v}{d}$ atque $m = \frac{bv}{cd} - \frac{v}{c} = \frac{\beta v}{d}$ ob $b = \beta c + d$. Quo autem valores ipsius m facilius reperiantur, primo valor ipsius A per B, tum valor ipsius B per C et ita porro exprimi debet, unde nata est ista tabula:

1. $m = \frac{Ab - v}{c}$,
2. $m = \frac{Bb + \beta v}{d}$,
3. $m = \frac{Cb - v(1 + \beta\gamma)}{e}$,
4. $m = \frac{Db + v(\delta + \beta\gamma\delta + \beta)}{f}$,
5. $m = \frac{Eb - v(\delta\varepsilon + \beta\gamma\delta\varepsilon + \beta\varepsilon + \beta\gamma + 1)}{g}$,
6. $m = \frac{Fb + v(\delta\varepsilon\zeta + \beta\gamma\delta\varepsilon\zeta + \beta\varepsilon\zeta + \beta\gamma\zeta + \zeta + \delta + \beta\gamma\delta + \beta)}{h}$

etc.

De his valoribus est notandum signa ipsius v alternari hoc modo $-+-+-+$ etc. Deinde coefficientes ipsius v hanc tenent legem

$$\begin{array}{cccccc} \beta & \gamma & \delta & \varepsilon & \zeta & \\ 1, & \beta, & \beta\gamma+1, & \beta\gamma\delta+\delta+\beta, & \beta\gamma\delta\varepsilon+\delta\varepsilon+\beta\varepsilon+\beta\gamma+1 & \text{etc.,} \end{array}$$

cuius progressionis quisque terminus est aggregatum ex termino praecedente in indicem supra se scriptum multiplicato et termino hunc praecedente.

9. Si igitur v per b dividi poterit, erit $m=0$; si v per c dividi potest, erit $m=\frac{-v}{c}$ propter $A=0$; si v per d dividi poterit, fiat $B=0$ eritque $m=\frac{v}{d}\beta$. Unde sequens oritur lex:

Si est numerus integer	erit
$\frac{v}{b}$	$m=0$
$\frac{v}{c}$	$m=-\frac{v}{c}$
$\frac{v}{d}$	$m=+\frac{v}{d}\beta$
$\frac{v}{e}$	$m=-\frac{v}{e}(\beta\gamma+1)$
$\frac{v}{f}$	$m=+\frac{v}{f}(\beta\gamma\delta+\delta+\beta)$
$\frac{v}{g}$	$m=-\frac{v}{g}(\beta\gamma\delta\varepsilon+\delta\varepsilon+\beta\varepsilon+\beta\gamma+1)$
$\frac{v}{h}$	$m=+\frac{v}{h}(\beta\gamma\delta\varepsilon\zeta+\delta\varepsilon\zeta+\beta\varepsilon\zeta+\beta\gamma\zeta+\beta\gamma\delta+\zeta+\delta+\beta)$
	etc.

Si nunc hi ipsius m valores in aequatione $z=ma+p$ substituantur, reperietur, ut sequitur:

Si est integer	erit
$\frac{v}{b}$	$z = q + \frac{bv}{b}1 = q + v$
$\frac{v}{c}$	$z = q - \frac{bv}{c}\alpha$
$\frac{v}{d}$	$z = q + \frac{bv}{d}(\alpha\beta + 1)$
$\frac{v}{e}$	$z = q - \frac{bv}{e}(\alpha\beta\gamma + \alpha + \gamma)$
$\frac{v}{f}$	$z = q + \frac{bv}{f}(\alpha\beta\gamma\delta + \alpha\beta + \alpha\delta + \gamma\delta + 1)$
$\frac{v}{g}$	$z = q - \frac{bv}{g}(\alpha\beta\gamma\delta\varepsilon + \alpha\beta\gamma + \alpha\beta\varepsilon + \alpha\delta\varepsilon + \gamma\delta\varepsilon + \alpha + \gamma + \varepsilon)$

etc.

10. Ad inveniendum ergo numerum z, qui per a divisus relinquat p et per b divisus relinquat q, posito $p - q = v$ sequentem habebimus regulam:

Instituatur operatio ad maximum communem divisorem inter a et b inveniendum eaque eousque producatur, donec ad residuum perveniatur, quod sit divisor ipsius v, teneaturque quotus ex divisione ipsius v per illud residuum resultans, qui sit Q, ubi operatio abrumpatur. Deinde in serie scribantur quoti α, β, γ etc. in hac divisione orti ex iisque construatur nova series

$$1, \quad \alpha, \quad \alpha\beta + 1, \quad \alpha\beta\gamma + \alpha + \gamma \quad \text{etc.},$$

quae ex illa quotorum serie formatur atque eousque continuari debet, quousque per illam seriem fieri potest. Sub hac nova serie scribantur signa alternantia $+ - + -$ etc. ultimusque terminus cum suo signo multiplicetur per Q atque etiam per minorem divisorem propositum b; ad factum addatur residuum q divisori b respondens. Quo facto erit aggregatum numerus quaesitus.

11. Invento hoc modo uno numero satisfaciente z ex eo statim innumerabiles alii numeri satisfacientes reperiuntur. Nam si z per a divisum p relinquit et per b divisum q, eandem proprietatem habebunt quoque numeri $ab + z$, $2ab + z$ et $mab + z$. Multiplum quidem facti ab continuo adiici vel

auferri potest, si a et b fuerint inter se numeri primi; at si a et b fuerint numeri compositi, tum etiam sufficit eorum minimum communem dividuum sumsisse, cuius multiplum quodque adiectum vel ablatum a z dabit numeros satisfacientes; ut si minimus communis dividuus fuerit M, comprehendet $mM + z$ omnes omnino numeros quaestioni satisfacientes. Quare etiamsi hoc modo saepe numeri negativi pro z inveniantur, tamen adiiciendo ad eos M vel eius multiplum obtinebuntur numeri affirmativi. Hac ergo operatione semper minimus numerus satisfaciens invenietur, siquidem minimus communis dividuus M toties subtrahatur, quoties fieri potest.

12. Quia exemplis haec operatio maxime illustrabitur, quaeramus numerum, qui per 103 divisus relinquat 87 et per 57 divisus relinquat 25. Erit ergo $a = 103$, $b = 57$, $p = 87$ et $q = 25$ atque $v = 62$; quare operationem ita instituo:

$$\begin{array}{r|r|l}
57 & 103 & 1 \\
 & 57 & \\
\hline
46 & 57 & 1 \\
 & 46 & \\
\hline
11 & 46 & 4 \\
 & 44 & \\
\hline
 & 2 &
\end{array}
\qquad \frac{62}{2} = 31 = Q$$

$$\begin{array}{cccc}
1 & 1 & 4 & \\
1, & 1, & 2, & 9 \\
+ & - & + & -
\end{array}$$

Nunc est $-9 \cdot 31 = -279$ atque numerus quaesitus $= 25 - 57 \cdot 279$; qui cum fiat negativus, addo ad eum $3 \cdot 57 \cdot 103$ seu $57 \cdot 309$, unde invenitur $25 + 57 \cdot 30 = 1735$, qui est minimus numerus quaesitus; omnes vero satisfacientes continentur in hac forma $m \cdot 103 \cdot 57 + 1735$.

13. Quaeramus porro numerum, qui per 41 divisus relinquat 10 et per 29 divisus relinquat 28. In hoc exemplo compendium adhibebo, quod in aliis similibus computationibus magnam habebit utilitatem; nam cum in divisione per 29 residuum sit 28, restare quoque poterit in eadem divisione -1, si quotus unitate maior accipiatur. Sumo ergo -1 pro residuo divisoris 29

eritque $a = 41$, $b = 29$, $p = 10$ et $q = -1$, unde erit $v = 11$. Operationem ergo ut ante instituo ita:

```
29 | 41 | 1
   | 29 |
   ------
     12 | 29 | 2
        | 24 |
        ------
           5 | 12 | 2
             | 10 |
             ------
                2 | 5 | 2
                  | 4 |
                  -----
                    1
```

$$\tfrac{11}{1} = 11 = Q$$

1	2	2	2	
1,	1,	3,	7,	17
+	−	+	−	+

Erit ergo $+17 \cdot 11 = 187$ atque numerus quaesitus $= -1 + 29 \cdot 187$. Subtrahatur $29 \cdot 4 \cdot 41$; erit is $= -1 + 29 \cdot 23 = 666$. Satisfacient ergo quaestioni omnes numeri in hac forma $m \cdot 41 \cdot 29 + 666$ contenti.

14. Compendium hinc se prodit ad supra datam regulam adiiciendum, quod in hoc constat, ut, postquam numerus Q per ultimum seriei formatae terminum est multiplicatus, factum per maiorem divisorem a dividatur atque residuum loco ipsius facti adhibeatur. Scilicet hoc residuum per minorem divisorem b multiplicatum atque residuo q auctum dabit numerum quaesitum. Atque iste numerus hoc pacto inventus erit minimus, qui satisfacit. Praeterea hac divisione effici potest, ut residuum prodeat affirmativum, etiamsi dividendus fuerit negativus. Ita in primo exemplo § 12 habebatur -279, qui numerus per 103 divisus sumto quoto $= 3$ relinquit $+30$. Ex quo numerus quaesitus minimus est $= 25 + 57 \cdot 30 = 1735$.

15. Fieri deinde etiam potest, ut huiusmodi exempla proponantur, quae solutionem omnino non admittant, uti si quaeratur numerus, qui per 24 divisus relinquat 13, per 15 vero divisus relinquat 9; talis enim numerus per alteram conditionem deberet esse per 3 divisibilis, per alteram secus. Idem

vero etiam ipsa regula ostendit; nunquam enim ad tale residuum excepto 0 devenietur, quod dividat v seu 4, uti ex ipsa operatione videre est:

15	24	1			
	15				
	9	15	1		
		9			
		6	9	1	
			6		
			3	6	2
				6	
				0	

Huiusmodi vero exempla exhiberi non possunt, nisi divisores a et b sint numeri compositi inter se; nam si fuerint inter se primi, semper numeri quaesiti exhiberi possunt. Sin autem divisores a et b fuerint numeri compositi atque v non dividi potuerit per maximum ipsorum a et b divisorem, tum semper problema ad absurdum deducit. Hocque est criterium, ex quo, num problema solutionem admittat, diiudicari potest, antequam operatio instituatur.

16. Exposita hac methodo universali, qua omnis generis huius problemata facile resolvi possunt, ex ea alia regula potest formari, quae quidem ad usum non est tam facilis, at simplicitatis plus in se habet. Oritur ea autem, si in valoribus supra inventis ipsius z (§ 9) loco α, β, γ etc. eorum valores ex aequationibus $a = \alpha b + c$, $b = \beta c + d$ etc. substituantur. Nam si instituatur operatio ad maximum communem divisorem inter a et b inveniendum ex eaque innotescant continua residua c, d, e etc., dico fore numerum

$$z = q + abv\left(\frac{1}{ab} - \frac{1}{bc} + \frac{1}{cd} - \frac{1}{de} + \frac{1}{ef} - \text{etc.}\right)$$

eousque hac serie continuanda, donec v per factorem aliquem denominatoris dividi queat.

Uti si quaeratur numerus, qui per 16 divisus relinquat 1 et per 9 divisus relinquat 7, erit $a = 16$, $b = 9$, $p = 1$, $q = 7$ et $v = -6$. Quare

$$\begin{array}{l} 9 \,|\, 16 \,|\, 1 \\ \ \ 9 \\ \hline \ 7 \,|\, 9 \,|\, 1 \\ \ 7 \\ \hline \ 2 \,|\, 7 \,|\, 3 \\ \ 6 \\ \hline \ 1 \end{array}$$

Hinc ergo erit

$$z = 7 - 6 \cdot 9 \cdot 16 \left(\frac{1}{16 \cdot 9} - \frac{1}{9 \cdot 7} + \frac{1}{7 \cdot 2}\right) = 7 - 6 + \frac{6 \cdot 16}{7} - \frac{3 \cdot 9 \cdot 16}{7} = 1 - 3 \cdot 16 = -47.$$

Satisfaciunt ergo omnes numeri $m \cdot 144 - 47$ seu $m \cdot 144 + 97$ eorumque minimus est 97.

Superior formula generalis ipsius z etiam in hunc modum potest exprimi

$$z = p - abv\left(\frac{1}{bc} - \frac{1}{cd} + \frac{1}{de} - \frac{1}{ef} + \text{etc.}\right),$$

quae series fractionum eousque continuari debet, donec valor ipsius z fiat numerus integer.

17. Considerabo nunc quosdam casus particulares, in quibus a ad b datam habeat relationem; et primo quidem sit $b = a - 1$ seu $a = b + 1$, residua vero ex divisione numeri quaesiti per a et b orta sint ut ante p et q. Erit ergo $c = 1$ ideoque per regulam postremam

$$z = p - av = p - ap + aq.$$

Quae expressio, si $aq + p > ap$, dat minimum numerum quaesito satisfacientem; at si $aq + p < ap$, tum minimus numerus satisfaciens erit $a^2 - a + p - ap + aq$. Omnes vero numeri satisfacientes in hac formula generali $ma^2 - ma + p - ap + aq$ comprehenduntur, seu etiam in ista $mb^2 + mb - bp + bq + q$. Quicquid nunc sit m, si haec quantitas dividatur per $b^2 + b$, residuum erit minimus numerus quaesito satisfaciens.

18. Quemadmodum hac ratione ope residuorum datorum, quae post divisionem numeri incogniti per divisores b et $b + 1$ remanent, ipse numerus

4*

incognitus sit inveniendus, docuit STIFELIUS[1]) in Commentario ad RUDOLFI artem Cossicam. Regula eius ita se habet: Si fuerit residuum numeri incogniti per $b+1$ divisi p et residuum eiusdem per b divisi q, iubet q multiplicare per $b+1$ et p per b^2 horumque factorum aggregatum per b^2+b dividere; quod restat post divisionem, id pronunciat esse numerum quaesitum. Fluit autem haec regula ex nostra generali formula, si ponatur $m=p$; tum enim habetur $b^2p+(b+1)q$, quod per b^2+b divisum relinquit minimum numerum quaesitum.

19. Interim tamen minori opera minimus numerus satisfaciens reperietur sequenti modo: Residuum q, quod ex divisione quaesiti numeri per b oritur, multiplicetur per $b+1$ factumque addatur ad numerum pronicum ipsius b, puta ad b^2+b, hinc subtrahatur factum ex residuo p, quod ex divisione numeri quaesiti per $b+1$ remanet, ducto in b; si id, quod restat, fuerit $< b^2+b$, erit id ipse numerus quaesitus, sin vero fuerit $> b^2+b$, subtrahatur b^2+b eritque residuum numerus quaesitus. Ut si quaeratur numerus, qui per 100 divisus relinquat 75 et per 101 divisus 37; tum addatur 10100 ad factum ex 75 in 101 seu 7575, ut habeatur 17675, hinc subtrahatur factum ex 37 in 100 seu 3700; remanebit 13975; a quo si 10100 auferantur, prodibit 3875, qui est minimus numerus quaesitus.

20. Si quaeratur numerus, qui per b divisus relinquat q et per $nb+1$ divisus p, erit iterum $c=1$ atque numerus quaesitus

$$z=p-av=p-ap+aq=(nb+1)q-nbp$$

ob $a=nb+1$. Atque omnes numeri satisfacientes continebuntur in hac expressione $mnb^2+mb+(nb+1)q-nbp$, ex qua sumto pro m numero quocunque invenietur minimus numerus satisfaciens, si ea expressio dividatur per nb^2+b; residuum enim erit minimus numerus satisfaciens.

21. Casus porro notari meretur, quo residua p et q, quae oriuntur ex divisione quaesiti numeri per datos divisores a et b, sunt inter se aequalia seu $p=q$. Hoc enim casu fit $v=0$ ideoque invenitur numerus quaesitus

1) M. STIFEL (1487—1567), *Die Coss CHRISTOFFS RUDOLFFS*, Königsperg 1553, fol. 16ʳ. Vide etiam M. STIFEL, *Arithmetica integra*, Norimbergae 1544, fol. 38ᵛ. F. R.

$z = p$. Si igitur sit M minimus communis dividuus numerorum a et b, omnes numeri satisfacientes continebuntur in hac formula $mM + p$. Eadem plane formula quoque satisfacit, si quotcunque fuerint divisores a, b, c, d etc., per quos singulos numerus quaesitus divisus relinquat p, si quidem M denotet omnium divisorum minimum communem dividuum. Omnes ergo numeri huiusmodi quaestionibus satisfacientes ita sunt comparati, ut per M divisi relinquant p.

22. Hinc satis tritum problema, quo quaeritur numerus, qui per 2, 3, 4, 5, 6 divisus relinquat 1, per 7 vero nihil relinquat, solvi potest. Omnes enim numeri, qui per 2, 3, 4, 5, 6 divisi relinquunt 1, hanc habent proprietatem, ut per 60, qui numerus est minimus communis dividuus numerorum 2, 3, 4, 5 et 6, divisi relinquant 1. Problema ergo huc redit, ut inveniatur numerus, qui per 60 divisus relinquat 1, per 7 vero sit divisibilis; erit ergo $a = 60$, $b = 7$, $p = 1$, $q = 0$ et $v = 1$. Facta ergo operatione

$$\begin{array}{llllllll} 7 & | \; 60 \; | & 8 & & & & & \\ & | \; 56 \; | & & & & & & \frac{1}{1} = 1 = Q \\ & 4 & | \; 7 \; | & 1 & & & & \\ & & | \; 4 \; | & & & & & \\ & & 3 & | \; 4 \; | & 1 & & & 8 \quad 1 \quad 1 \\ & & & | \; 3 \; | & & & & 1, \; 8, \; 9, \; 17 \\ & & & 1 & & & & + \; - \; + \; - \end{array}$$

erit $z = 0 - 119 + 420m$, et si $m = 1$, erit $z = 301$.

23. Maiorem difficultatem habere videtur hoc problema, quo quaeritur numerus, qui per numeros 2, 3, 4, 5, 6 divisus respective relinquat numeros 1, 2, 3, 4, 5, at per 7 dividi queat, propter residua proposita inaequalia. Sed haec quaestio congruit cum hac: Invenire numerum, qui per 2, 3, 4, 5, 6 divisus relinquat -1 et per 7 nihil. Illi iam conditioni satisfacit forma $60m - 1$; quare numerus quaeritur, qui per 60 divisus -1, at per 7 nihil relinquat; fit itaque $a = 60$, $b = 7$, $p = -1$, $q = 0$ et $v = -1$ atque operatione ut ante instituta est $Q = -1$, quod in -17 ductum dat $+17$; hocque per b multiplicatum dat 119, numerum quaesitum.

24. Ex his duobus exemplis apparet, quomodo huiusmodi quaestiones, in quibus quotcunque divisores proponuntur, quibus autem duo tantum residua

respondent, per supra datas regulas solvi queant; statim enim quaestio ad quaestionem duorum divisorum reducitur; uti si omnia residua sunt aequalia, quaestio perinde solvitur, ac si unicus divisor fuisset propositus. At si residua sunt inaequalia, tum nihilominus repetendis his operationibus, quibus pro duobus divisoribus usi sumus, solutio poterit obtineri. Primo enim duobus divisoribus satisfieri debet, tum tertius assumitur, deinde quartus, donec omnibus erit satisfactum. Hoc vero commodissime exemplis explicabitur.

25. Quaeramus igitur numerum, qui per 7 divisus relinquat 6, per 9 relinquat 7, per 11 relinquat 8 et per 17 relinquat 1. Ex his iam quatuor conditionibus sumamus duas quasque, ut duas priores, et investigemus omnes numeros iis satisfacientes. Erit ergo $a=9$, $b=7$, $p=7$, $q=6$ et $v=1$, quare operatio instituetur, uti sequitur:

7	9	1		$Q=1$
	7			
	2	7	3	1 3
		6		1, 1, 4
		1		+ − +

fietque $z=6+1\cdot 4\cdot 7=34.$

Omnes ergo numeri his duabus conditionibus satisfacientes continentur in hac forma $63m+34$ seu ita erunt comparati, ut per 63 divisi relinquant 34.

26. Problema ergo huc est reductum, ut inveniatur numerus, qui divisus per 63 relinquat 34, per 11 relinquat 8 et per 17 relinquat 1. Harum trium conditionum sumantur duae priores eritque $a=63$, $b=11$, $p=34$, $q=8$ et $v=26$, unde fluit sequens operatio:

11	63	5			
	55				$Q=\frac{26}{2}=13$
	8	11	1		
		8			
		3	8	2	5 1 2
			6		1, 5, 6, 17
			2		+ − + −

ergo $z=m\cdot 63\cdot 11+8-13\cdot 17\cdot 11.$

Quo minimus numerus satisfaciens reperiatur, ponatur $m = 4$; erit

$$z = 8 + 31 \cdot 11 = 349.$$

Omnes ergo numeri satisfacientes in hac continentur forma $693m + 349$ seu hanc habebunt proprietatem, ut per 693 divisi relinquant 349.

27. Problema ergo tandem huc est reductum, ut definiatur numerus, qui per 693 divisus relinquat 349 et per 17 divisus relinquat 1. Facio ergo $a = 693$, $b = 17$, $p = 349$, $q = 1$ et $v = 348$ sequentemque iuxta data praecepta instituo operationem:

$$\begin{array}{r|c|l} 17 & 693 & 41 \\ & 697 & \\ \hline -4 & & \end{array} \qquad Q = \frac{348}{-4} = -87.$$

$$\begin{array}{cc} & 41 \\ 1, & 41 \\ + & - \end{array}$$

$$z = 693 \cdot 17 \cdot m + 1 + 41 \cdot 87 \cdot 17.$$

Quo minimus numerus satisfaciens prodeat, pono $m = -5$ eritque

$$z = 1 + 102 \cdot 17 = 1735,$$

qui est minimus numerus quatuor praescriptis conditionibus satisfaciens. Omnes autem, qui satisfaciunt, hac continentur formula $11781m + 1735$. Ex hoc exemplo ergo abunde intelligitur, quomodo omnes huiusmodi quaestiones sint resolvendae.

28. Pertinet huc solutio problematis chronologici satis cogniti, quam, prout ex his regulis inveni, apponam, in quo annus a Christo nato quaeritur ex datis cyclis solis et lunae una cum indictione Romana illius anni. Cum enim cyclus solis sit residuum, quod oritur divisione numeri anni novenario aucti per 28, cyclus vero lunae sit residuum, quod oritur divisione numeri anni unitate aucti per 19, indictio vero Romana sit residuum, quod oritur, si numerus anni ternario auctus per 15 dividatur, sequens prodiit solutio. Sit p cyclus solis, q cyclus lunae et r indictio Romana; multiplicetur p per 4845, q per 4200 et r per 6916, haec tria producta cum numero 3267 in unam summam coniiciantur eaque dividatur per 7980; quod remanebit resi-

duum, erit numerus anni quaesiti. Si annus periodi Iulianae requiratur, tum operatio eodem modo instituatur, nisi quod numerus 3267 negligi debet; quae est regula iam passim tradita.

29. Multam quidem operam requirit solutio pro pluribus divisoribus, si quidem problema continuo ad casum, quo divisorum numerus unitate minuitur, ut in praecedente exemplo fecimus, reducitur; at ex ea ipsa operatione facilior multoque brevior via sese prodit, qua statim proposita quaestio, quotcunque etiam fuerint divisores, ad casum duorum divisorum reduci potest; quae regula ita se habet:

Inveniendus sit numerus, qui per divisores a, b, c, d, e, quos numeros inter se primos esse pono, divisus relinquat respective haec residua p, q, r, s, t. Huic quaestioni satisfacit iste numerus

$$Ap + Bq + Cr + Ds + Et + mabcde,$$

in qua expressione A est numerus, qui per factum $bcde$ divisus nihil relinquat, per a vero divisus relinquat unitatem; B est numerus, qui per $acde$ divisus relinquat nihil, per b vero unitatem; C est numerus, qui per $abde$ divisus nihil relinquat, per c vero unitatem; D est numerus, qui per $abce$ divisus nihil relinquat, per d vero unitatem; atque E est numerus, qui per $abcd$ divisus nihil relinquat, per e vero unitatem; qui ergo numeri per regulam pro duobus divisoribus datam inveniri possunt.

THEOREMATUM QUORUNDAM AD NUMEROS PRIMOS SPECTANTIUM DEMONSTRATIO[1]

Commentatio 54 indicis ENESTROEMIANI
Commentarii academiae scientiarum Petropolitanae 8 (1736), 1741, p. 141–146

1. Plurima quondam a FERMATIO theoremata arithmetica, sed sine demonstrationibus in medium sunt prolata, in quibus, si vera essent, non solum eximiae numerorum proprietates continerentur, verum etiam ipsa numerorum scientia, quae plerumque Analyseos limites excedere videtur, vehementer esset promota. Quamvis autem iste insignis Geometra de pluribus, quae proposuit, theorematis asseruerit se ea vel demonstrare posse vel saltem de eorum veritate esse certum, tamen nusquam, quantum mihi constat, demonstrationes exposuit. Quin potius FERMATIUS videtur maximam theorematum suorum numericorum partem per inductionem esse assecutus, quippe quae via fere unica ad huiusmodi proprietates eruendas patere videatur. At vero quam parum inductionibus in hoc negotio tribui possit, pluribus exemplis possem declarare; ex quibus autem unicum ab ipso FERMATIO desumtum attulisse sufficiat. Loquor nimirum de illo theoremate, cuius falsitatem iam aliquot ab hinc annis ostendi, quo FERMATIUS asserit omnes numeros hac forma $2^{2^n}+1$ comprehensos esse numeros primos.[2]) Ad veritatem autem huius propositionis evincendam inductio omnino sufficere videtur. Nam praeterquam quod omnes isti numeri minores quam 100000 sint revera primi, demonstrari etiam facile potest nullum numerum primum 600 non excedentem hanc formulam $2^{2^n}+1$, quantumvis magnus etiam numerus pro n substituatur,

1) Vide etiam Commentationes 134 et 262 huius voluminis. F. R.

2) Vide Commentationem 26 huius voluminis. F. R.

metiri. Cum tamen nihilominus constet hanc propositionem veritati non esse consentaneam, facile intelligitur, quantum inductio in huiusmodi speculationibus valeat.

2. Hanc ob rationem omnes huiusmodi numerorum proprietates, quae sola inductione nituntur, tam diu pro incertis habendas esse arbitror, donec illae vel apodicticis demonstrationibus muniantur vel omnino refellantur. Non plus etiam illis theorematis, quae ego ipse illi schediasmati, in quo de memorato theoremate FERMATIANO numerisque perfectis tractavi, subieci, fidendum esse censerem, si tantum inductionibus, qua via quidem sola tum temporis ad eorum cognitionem perveni, niterentur. Nunc vero, postquam peculiari methodo demonstrationes horum theorematum firmissimas sum adeptus, de veritate eorum non amplius est dubitandum. Quocirca tam ad veritatem illorum theorematum ostendendam quam ad methodum ipsam, qua demonstrationes has inveni, exponendam,[1]) quae forte etiam in aliis numerorum investigationibus utilitatem afferre poterit, in hac dissertatione meas demonstrationes explicare constitui.

3. Propositio autem, quam hic demonstrandam suscepi, est sequens:

Significante p numerum primum formula $a^{p-1}-1$ semper per p dividi poterit, nisi a per p dividi queat.[2])

Ex hac enim propositione demonstrata sponte reliquorum theorematum veritas fluit. Casum quidem formulae propositae, quo est $a=2$, iam ab aliquo tempore demonstratum dedi[3]); attamen tum demonstrationem ad generalem formulam extendere non licuit. Quamobrem primo huius casus probationem afferre conveniet, quo transitus ad generaliora eo facilior reddatur. Demonstranda igitur erit sequens propositio:

Significante p numerum primum imparem quemcunque formula $2^{p-1}-1$ semper per p dividi poterit.

---

1) In editione principe manuscripti verba *qua demonstrationes has inveni, exponendam,* omissa sunt. F. R.

2) Hoc celebre theorema, quod ab inventore theorema FERMATIANUM nominari solet, FERMATIUS epistola d. d. 18. Octobris a. 1640 cum FRENICLIO sine demonstratione communicavit. Vide P. DE FERMAT, *Varia opera mathematica,* Tolosae 1679, p. 162; *Oeuvres DE FERMAT,* t. II, p. 206.

De demonstratione theorematis FERMATIANI ante EULERUM a LEIBNIZIO data vide G. VACCA, *Intorno alla prima dimostrazione di un teorema di FERMAT,* Biblioth. Mathem. 8_2, 1894, p. 46, et D. MAHNKE, *LEIBNIZ auf der Suche nach einer allgemeinen Primzahlgleichung,* Biblioth. Mathem. 13_3, 1912/3, p. 29. F. R. 3) Vide p. 3—4. F. R.

DEMONSTRATIO

Loco 2 ponatur $1+1$ eritque

$$(1+1)^{p-1}=1+\frac{p-1}{1}+\frac{(p-1)(p-2)}{1\cdot 2}+\frac{(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3}+\frac{(p-1)(p-2)(p-3)(p-4)}{1\cdot 2\cdot 3\cdot 4}+\text{etc.},$$

cuius seriei terminorum numerus est $=p$ et proinde impar. Praeterea quilibet terminus, quamvis habeat fractionis speciem, dabit numerum integrum; quisque enim numerator, uti satis constat, per suum denominatorem dividi potest. Demto igitur seriei termino primo 1 erit

$$(1+1)^{p-1}-1=2^{p-1}-1$$
$$=\frac{p-1}{1}+\frac{(p-1)(p-2)}{1\cdot 2}+\frac{(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3}+\frac{(p-1)(p-2)(p-3)(p-4)}{1\cdot 2\cdot 3\cdot 4}+\text{etc.},$$

quorum numerus est $=p-1$ et propterea par. Colligantur igitur bini quique termini in unam summam, quo terminorum numerus fiat duplo minor; erit

$$2^{p-1}-1=\frac{p(p-1)}{1\cdot 2}+\frac{p(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3\cdot 4}$$
$$+\frac{p(p-1)(p-2)(p-3)(p-4)(p-5)}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6}+\text{etc.},$$

cuius seriei ultimus terminus ob p numerum imparem erit

$$\frac{p(p-1)(p-2)\cdots 2}{1\cdot 2\cdot 3\cdots(p-1)}=p.$$

Apparet autem singulos terminos per p esse divisibiles; nam cum p sit numerus primus et maior quam ullus denominatorum factor, nusquam divisione tolli poterit. Quamobrem si fuerit p numerus primus impar, per illum semper $2^{p-1}-1$ dividi poterit. Q. E. D.

ALITER

Si $2^{p-1}-1$ per numerum primum p dividi potest, dividi quoque poterit eius duplum 2^p-2 et vicissim. At est

$$2^p=(1+1)^p=1+\frac{p}{1}+\frac{p(p-1)}{1\cdot 2}+\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}+\cdots+\frac{p}{1}+1.$$

Quae series terminis primo et ultimo truncata dat

$$\frac{p}{1}+\frac{p(p-1)}{1\cdot 2}+\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}+\cdots+\frac{p(p-1)}{1\cdot 2}+p=2^p-2.$$

Perspicuum autem est istius seriei quemvis terminum per p esse divisibilem, siquidem p fuerit numerus primus. Quamobrem etiam semper 2^p-2 per p et propterea quoque $2^{p-1}-1$ per p dividi poterit, nisi sit $p=2$. Q. E. D.

4. Cum igitur $2^{p-1}-1$ per numerum primum imparem p dividi queat, facile intelligitur per p quoque dividi posse hanc formulam $2^{m(p-1)}-1$ denotante m numerum quemcunque integrum. Quare sequentes formulae quoque omnes $4^{p-1}-1$, $8^{p-1}-1$, $16^{p-1}-1$ etc. per numerum primum p dividi poterunt. Demonstrata igitur est veritas theorematis generalis pro omnibus casibus, quibus a est quaevis binarii potestas et p quicunque numerus primus praeter binarium.

5. Demonstrato nunc hoc theoremate eius ope sequens quoque demonstrabimus

THEOREMA

Denotante p numerum primum quemcunque praeter 3 per illum semper haec formula $3^{p-1}-1$ dividi poterit.

DEMONSTRATIO

Si $3^{p-1}-1$ per numerum primum p excepto 3 dividi potest, tum 3^p-3 per p dividi poterit, quoties p fuerit numerus primus quicunque, et vicissim. Est vero

$$3^p=(1+2)^p=1+\frac{p}{1}\cdot 2+\frac{p(p-1)}{1\cdot 2}\cdot 4+\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}\cdot 8+\cdots+\frac{p}{1}\cdot 2^{p-1}+2^p,$$

cuius seriei singuli termini praeter primum et ultimum per p dividi poterunt, si quidem p fuerit numerus primus. Per p igitur dividi potest ista formula 3^p-2^p-1, quae aequalis est huic

$$3^p-3-2^p+2.$$

At 2^p-2 semper per p numerum primum dividi potest; ergo etiam 3^p-3.

Quare $3^{p-1}-1$ semper per p dividi potest, quoties p fuerit numerus primus excepto 3. Q. E. D.

6. Eodem modo ulterius progredi liceret ab hoc ipsius a valore ad sequentem unitate maiorem. Sed quo demonstrationem generalis theorematis magis concinnam magisque genuinam efficiam, sequens praemitto

THEOREMA

Denotante p numerum primum si a^p-a per p dividi potest, tum per idem p quoque formula $(a+1)^p-a-1$ dividi poterit.

DEMONSTRATIO

Resolvatur $(1+a)^p$ consueto more in seriem; erit

$$(1+a)^p=1+\frac{p}{1}a+\frac{p(p-1)}{1\cdot 2}a^2+\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}a^3+\cdots+\frac{p}{1}a^{p-1}+a^p,$$

cuius seriei singuli termini per p dividi possunt praeter primum et ultimum, si quidem p fuerit numerus primus. Quamobrem $(1+a)^p-a^p-1$ divisionem per p admittet; haec autem formula congruit cum hac $(1+a)^p-a-1-a^p+a$. At a^p-a per hypothesin per p dividi potest, ergo et $(1+a)^p-a-1$. Q. E. D.

7. Cum igitur, posito quod a^p-a per p numerum primum dividi queat, per p quoque haec formula $(a+1)^p-a-1$ divisionem admittat, sequitur etiam $(a+2)^p-a-2$, item $(a+3)^p-a-3$ et generaliter $(a+b)^p-a-b$ per p dividi posse. Posito autem $a=2$, quia 2^p-2, uti iam demonstravimus, per p dividi potest, perspicuum est formulam $(b+2)^p-b-2$ divisionem per p admittere debere, quicunque integer numerus loco b substituatur.

Metietur ergo p formulam a^p-a et consequenter etiam hanc[1]) $a^{p-1}-1$, nisi fuerit $a=p$ vel multiplo ipsius p. Atque haec est demonstratio generalis theorematis, quam tradere suscepi.

1) In editione principe manuscripti verba a^p-a *et consequenter etiam hanc* omissa sunt. F. R.

THEOREMATUM QUORUNDAM ARITHMETICORUM DEMONSTRATIONES

Commentatio 98 indicis ENESTROEMIANI
Commentarii academiae scientiarum Petropolitanae 10 (1738), 1747, p. 125—146

Theoremata arithmetica, cuiusmodi FERMATIUS aliique plurima detexerunt, eo maiore attentione sunt digna, quo magis eorum veritas est abscondita et demonstratu difficilis. FERMATIUS quidem satis magnam talium theorematum copiam reliquit, nusquam autem demonstrationes exposuit, etiamsi firmiter asserat sibi de eorum veritate certissime constare. Maxime igitur dolendum est eius scripta adeo periisse, ut etiamnum omnes demonstrationes ignorentur. Similis quoque est ratio propositionum in vulgus notarum, quibus neque summam neque differentiam duorum biquadratorum quadratum constituere posse asseritur; quamvis enim de earum veritate nemo dubitet, tamen nusquam extat demonstratio, quantum mihi quidem constat, rigida, praeter libellum quemdam a FRENICLIO olim editum, cuius titulus est *Traité des triangles rectangles en nombres.*[1]) Demonstrat autem hic Autor inter alia in nullo triangulo rectangulo, cuius latera rationalibus exprimuntur numeris, aream posse esse quadratum[2]), unde facile veritas memoratarum propositionum de summa et differentia duorum biquadratorum deducitur. Sed ista demonstratio tantopere proprietatibus triangulorum est involuta, ut, nisi summa

1) B. FRÉNICLE DE BESSY (1605—1675), *Traité des triangles rectangles en nombres*, Paris 1676; Mém. de l'acad. d. sc. de Paris (1666—99), t. V, 1729, p. 127 (vide imprimis p. 174—178). F. R.

2) Hoc theorema FERMATIUS iam a. 1659 cum CARCAVIO communicaverat; vide *Oeuvres de Fermat*, t. I, p. 340, t. II, p. 431. Vide etiam G. WERTHEIM, *Ein von Fermat herrührender Beweis*, Zeitschr. f. Mathem. 44, 1899, Hist. Abt., p. 4, et G. ENESTROEM, Biblioth. Mathem. 4_3, 1903, p. 88. F. R.

attentio adhibeatur, vix perspicuè intelligi possit. Hanc ob rem operae pretium fore arbitror, si harum propositionum demonstrationes a triangulis rectangulis abstraxero easque analytice et clare proposuero. Eo maiorem autem hoc meum institutum afferet utilitatem, quo plura alia theoremata multo difficiliora ex iis elici possunt. Huc scilicet pertinet theorema illud celebre FERMATII, quo statuit nullum numerum trigonalem esse posse biquadratum praeter unitatem, cuius demonstrationem ex illis formare mihi contigit.[1]) Eo difficilior autem ista demonstratio videtur, cum propositio exceptioni sit obnoxia atque tantum ad numeros integros pertineat; numeris enim fractis infinitis modis effici potest, ut $\frac{x(x+1)}{2}$ fiat biquadratum. Ad hoc igitur aliaque nonnulla theoremata demonstranda necesse erit lemmata quaedam praemittere, quibus sequentes demonstrationes innituntur; ante autem monuisse oportet perpetuo omnes litteras mihi numeros integros designare.

LEMMA 1

Factum ex duobus pluribusve numeris inter se primis nec quadratum nec cubus nec ulla alia potestas esse potest, nisi singuli factores sint quadrata vel cubi vel eiusmodi aliae potestates.

Demonstratio huius lemmatis facilis est atque ab EUCLIDE[2]) iam est tradita, ita ut superfluum foret eam hic exponere.

LEMMA 2

Si a^2+b^2 fuerit quadratum atque a et b sint numeri inter se primi, erit $a=pp-qq$ et $b=2pq$ existentibus p et q numeris inter se primis altero pari, altero impari.

DEMONSTRATIO

Quia est a^2+b^2 quadratum, ponatur eius radix $=a+\frac{bq}{p}$, ubi fractionem $\frac{q}{p}$ in minimis terminis pono expressam, ita ut p et q sint numeri inter se primi.

1) Vide p. 51. F. R.

2) EUCLIDIS *Elementa* (ed. I. L. HEIBERG), vol. II, lib. VII prop. 30 (= 32 aliarum editionum). F. R.

Facta autem aequatione erit $a^2+b^2=a^2+\frac{2abq}{p}+\frac{bbqq}{pp}$. Unde fit

$$a:b=pp-qq:2pq.$$

Numeri autem $pp-qq$ et $2pq$ inter se vel primi sunt vel communem habent divisorem 2. Illo igitur casu, quo $pp-qq$ et $2pq$ sunt numeri inter se primi, quod accidit, si numerorum p et q alter fuerit par, alter impar, necesse est, ut sit

$$a=pp-qq \quad \text{et} \quad b=2pq,$$

quia a et b numeri ponuntur inter se primi. Casu autem, quo numeri $pp-qq$ et $2pq$ communem divisorem habent 2, quod erit, si numerorum p et q uterque fuerit impar (uterque enim par esse nequit, quia inter se ponuntur primi), erit $a=\frac{pp-qq}{2}$ et $b=pq$. Ponatur autem $p+q=2r$ et $p-q=2s$; erunt r et s numeri inter se primi eorumque alter par, alter impar, unde fit

$$a=2rs \quad \text{et} \quad b=rr-ss;$$

quae expressio, quia cum priore congruit, indicat, si $aa+bb$ fuerit quadratum et numeri a et b sint inter se primi, alterum eorum esse differentiam duorum quadratorum inter se primorum, quorum alter par est, alter impar, alterum vero numerum aequari duplici facto ex radicibus istorum quadratorum. Hoc est esse

$$a=pp-qq \quad \text{et} \quad b=2pq$$

existentibus p et q numeris inter se primis altero pari, altero impari. Q. E. D.

COROLLARIUM 1

Si ergo summa duorum quadratorum inter se primorum fuerit quadratum, alterum quadratum par sit necesse est, alterum vero impar; ex quo sequitur summam duorum quadratorum imparium non posse esse quadratum.

COROLLARIUM 2

Si ergo $aa+bb$ est quadratum, numerorum a et b alter, puta a, erit impar, alter b vero par. Impar vero a erit $=pp-qq$ et par $b=2pq$.

COROLLARIUM 3

Quia porro numerorum p et q alter est par, alter impar, erit b numerus pariter par seu per 4 divisibilis. Deinde si nec p nec q fuerit per 3 divisibilis, necesse est, ut vel $p-q$ vel $p+q$ divisionem per 3 admittat. Unde sequitur alterum numerorum a et b, quorum quadratorum summa facit quadratum, esse per 3 divisibilem.

COROLLARIUM 4

Cum sit $a = pp - qq$ et $b = 2pq$, si $aa + bb$ constituat quadratum, facile intelligitur numeros p et q minores esse quam a et b. Quoniam enim est $a = (p+q)(p-q)$, erit $a > p+q$, nisi $p-q$ sit $=1$; atque ob $b = 2pq$ erit b maior quam p vel q. Potiore ergo ratione numeri a et b maiores erunt quam numeri p et q. Fieret quidem $a = 0$, si foret $p = q$, sed hic casus locum non habet, quia p et q ponuntur numeri inter se primi eorumque alter par, alter impar.

SCHOLION

In demonstratione huius lemmatis ex analogia $a : b = pp - qq : 2pq$ ideo sequitur esse $a = pp - qq$ et $b = 2bq$, quia a et b sunt numeri inter se primi pariterque numeri $pp - qq$ et $2pq$. Si enim fuerit $a : b = c : d$ atque tam numeri a et b quam numeri c et d sint primi inter se, necesse est, ut sit $a = c$ et $b = d$, prout facile ex natura proportionum constat.

LEMMA 3

Si fuerit $aa - bb$ quadratum existentibus a et b numeris inter se primis, erit $a = pp + qq$ et vel $b = pp - qq$ vel $b = 2pq$, ubi numeri p et q sunt inter se primi eorumque alter par, alter impar.

DEMONSTRATIO

Quia $aa - bb$ est quadratum, ponatur $a^2 - b^2 = c^2$ eritque $a^2 = b^2 + c^2$ atque b et c numeri inter se primi. Cum igitur per Corollarium 1 lemmatis praecedentis numerorum b et c alter par sit, alter impar, necesse est, ut a sit numerus impar; b vero vel par erit vel impar.

Sit primo b impar et c par; erit per lemma praecedens $b = pp - qq$ et $c = 2pq$ existentibus p et q numeris inter se primis altero pari, altero impari. Hinc autem fit $a = pp + qq$. At si b fuerit par et c impar, erit $b = 2pq$ et $c = pp - qq$, unde denuo fit $a = pp + qq$. Quocirca si $aa - bb$ fuerit quadratum, erit

$$a = pp + qq \quad \text{atque vel} \quad b = pp - qq \quad \text{vel} \quad b = 2pq.$$

Q. E. D.

COROLLARIUM 1

Si ergo differentia duorum quadratorum est numerus quadratus, maius quadratum debet esse numerus impar, si quidem illa quadrata inter se fuerint numeri primi.

COROLLARIUM 2

Simili porro modo intelligitur numeros p et q minores esse quam numeros a et b, cum sit $a = pp + qq$ atque b vel $= pp - qq$ vel $= 2pq$.

COROLLARIUM 3

Si fuerit $aa - bb = cc$, unus numerorum a, b, c semper per 5 divisibilis existit. Nam cum sit $a = pp + qq$, $b = pp - qq$ et $c = 2pq$, vel alter numerorum p et q per 5 divisibilis est vel neuter; illo autem casu fit c divisibile per 5. Hoc vero casu erunt pp et qq numeri eiusmodi formae $5n \pm 1$, ergo vel $pp - qq$ vel $pp + qq$ per 5 divisibile erit.

THEOREMA 1

Summa duorum biquadratorum ut $a^4 + b^4$ non potest esse quadratum, nisi alterum biquadratum evanescat.

DEMONSTRATIO

In theoremate hoc demonstrando ita versabor, ut ostendam, si uno casu fuerit $a^4 + b^4$ quadratum, quantumvis etiam magni fuerint numeri a et b, tum continuo minores numeros loco a et b assignari posse atque tandem ad

minimos numeros integros perveniri oportere. Cum autem in minimis numeris tales non dentur, quorum biquadratorum summa quadratum constitueret, concludendum erit nec inter maximos numeros tales extare.

Ponamus ergo a^4+b^4 esse quadratum atque a et b inter se esse numeros primos; nisi enim primi forent, per divisionem ad primos reduci possent. Sit a numerus impar, b vero par, quia necessario alter par, alter impar esse debet. Erit ergo

$$aa=pp-qq \quad \text{et} \quad bb=2pq$$

numerique p et q inter se erunt primi eorumque alter par, alter impar. Cum autem sit $aa=pp-qq$, necesse est, ut p sit numerus impar, quia alias $pp-qq$ quadratum esse non posset. Erit ergo p numerus impar et q numerus par. Quia porro $2pq$ quadratum esse debet, necesse est, ut tam p quam $2q$ sit quadratum, quia p et $2q$ sunt numeri inter se primi. Ut vero $pp-qq$ sit quadratum, necesse est, ut sit

$$p=mm+nn \quad \text{et} \quad q=2mn$$

existentibus iterum m et n numeris inter se primis eorumque altero pari, altero impari. Sed quoniam $2q$ quadratum est, erit $4mn$ seu mn quadratum; unde tam m quam n quadrata erunt. Posito ergo

$$m=xx \quad \text{et} \quad n=yy$$

erit

$$p=m^2+n^2=x^4+y^4,$$

quod quadratum pariter esse deberet. Hinc ergo sequitur, si a^4+b^4 foret quadratum, tum quoque x^4+y^4 fore quadratum; manifestum autem est numeros x et y longe minores fore quam a et b. Pari igitur via ex biquadratis x^4+y^4 denuo minora orientur, quorum summa esset quadratum, atque pergendo ad minima tandem biquadrata in integris pervenietur. Cum ergo non dentur minima biquadrata, quorum summa efficeret quadratum, palam est nec in maximis numeris talia dari. Si autem in uno biquadratorum pari alterum sit $=0$, in omnibus reliquis paribus alterum evanescet, ita ut hinc nulli novi casus oriantur. Q. E. D.

COROLLARIUM 1

Cum igitur summa duorum biquadratorum non posset esse quadratum, multo minus duo biquadrata coniuncta biquadratum efficere poterunt.

COROLLARIUM 2

Quamquam demonstratio haec tantum ad numeros integros pertinet, tamen etiam per eam conficitur, ne in fractis quidem duo biquadrata exhiberi posse, quorum summa esset quadratum. Nam si $\frac{a^4}{m^4}+\frac{b^4}{n^4}$ foret quadratum, tum quoque in integris esset $a^4n^4+b^4m^4$ quadratum, quod fieri nequit per ipsam demonstrationem.

COROLLARIUM 3

Ex eadem demonstratione colligere licet non dari eiusmodi numeros p et q, ut p, $2q$ et $pp-qq$ sint quadrata; si enim tales existerent, tum haberentur valores pro a et b, qui redderent a^4+b^4 quadratum; foret namque $a=\sqrt{(pp-qq)}$ et $b=\sqrt{2pq}$.

COROLLARIUM 4

Positis ergo $p=xx$ et $2q=4yy$ erit $pp-qq=x^4-4y^4$. Fieri ergo omnino nequit, ut x^4-4y^4 sit quadratum. Neque igitur $4x^4-y^4$ quadratum esse poterit; foret enim quadratum $16x^4-4y^4$, qui casus ob $16x^4$ biquadratum ad priorem recidit.

COROLLARIUM 5

Sequitur hinc etiam $ab(a^2+b^2)$ quadratum nunquam esse posse. Ob factores enim a, b, a^2+b^2 inter se primos singulos quadrata esse oporteret, quod fieri nequit.

COROLLARIUM 6

Similiter tales etiam numeri inter se primi a et b non dabuntur, qui producerent $2ab(aa-bb)$ quadratum. Sequitur hoc ex Corollario 3, ubi monstratum est non dari numeros p et q, ut essent p, $2q$, $pp-qq$ quadrata. Haec omnia autem quoque valent pro numeris inter se non primis atque adeo fractis per Corollarium 2.

THEOREMA 2

Differentia duorum biquadratorum ut a^4-b^4 non potest esse quadratum, nisi sit vel $b=0$ vel $b=a$.

DEMONSTRATIO

Theorema hoc pari modo demonstrabo quo praecedens. Sint igitur biquadrata iam ad minimos terminos reducta atque ponamus a^4-b^4 esse quadratum; erit a numerus impar, b vero vel par erit vel impar.

CASUS 1

Sit primo b numerus par; erit

$$a^2=pp+qq \quad \text{et} \quad b^2=2pq$$

existentibus p et q inter se primis eorumque altero p pari, altero q impari. Ob $b^2=2pq$ debebunt ergo $2p$ et q esse quadrata. Quia porro $pp+qq$ ipsi a^2 aequatur, erit

$$q=mm-nn \quad \text{et} \quad p=2mn$$

existentibus m et n numeris inter se primis. Cum autem $2p$ sit quadratum, erit $4mn$, hoc est mn quadratum; adeoque m et n singillatim quadrata. Factis ergo

$$m=x^2 \quad \text{et} \quad n=y^2$$

fiet

$$q=x^4-y^4;$$

ubi cum numerorum m et n alter sit par, alter impar, erit quoque numerorum x et y alter par, alter impar. At ob q quadratum quadratum erit x^4-y^4, ubi x erit numerus impar, y vero par. Quocirca si fuerit a^4-b^4 quadratum, quadratum quoque erit x^4-y^4 existentibus x et y longe minoribus quam a et b. Cum ergo in minimis numeris non dentur duo biquadrata differentiam quadratum habentia, nec in maximis dabuntur, saltem casu, quo minus biquadratum est numerus par. Q. E. Unum.

CASUS 2

Sit nunc b numerus impar eritque

$$a^2=pp+qq \quad \text{et} \quad b^2=pp-qq$$

existentibus p et q numeris inter se primis eorumque altero pari, altero impari. Quia vero $pp-qq$ est quadratum, erit p numerus impar et propterea q par. Ductis autem a^2 et b^2 in se invicem prodibit $a^2b^2=p^4-q^4$, quae

expressio per casum primum quadratum esse ideoque ipsi a^2b^2 aequari non potest. Differentia ergo duorum biquadratorum nullo modo esse potest quadratum, nisi vel ambo sint aequalia vel minus $=0$. Q. E. Alterum D.

COROLLARIUM 1

Cum sit $a^2 = pp + qq$ et $b^2 = 2pq$ itemque $q = mm - nn$ et $p = 2mn$ atque porro $m = x^2$ et $n = y^2$, erit $a^2 = (x^4 + y^4)^2$ et $b^2 = 4x^2y^2(x^4 - y^4)$. Ex quo habebitur $a = x^4 + y^4$ et $b = 2xy\sqrt{(x^4 - y^4)}$.

COROLLARIUM 2

Si ergo in numeris exiguis x et y darentur tales, quorum biquadratorum differentia constitueret quadratum, tum ex iis statim multo maiores numeri eadem proprietate gaudentes a et b inveniri possent.

COROLLARIUM 3

Hinc clarius perspicitur casum, quo biquadrata vel sunt aequalia vel alterum $=0$, novos casus non praebere; facto enim vel $x = y$ vel $y = 0$ fit simul $b = 0$, unde vis demonstrationis eo magis percipitur.

COROLLARIUM 4

Ex demonstratione porro sequitur non dari numeros p et q eius indolis, ut essent $2p$, q et $pp + qq$ quadrata. Posito ergo $2p = 4xx$ et $q = yy$ non poterit esse quadratum ista forma $4x^4 + y^4$.

COROLLARIUM 5

Ex his formulis quoque sequitur nec $ab(aa - bb)$ nec $2ab(aa + bb)$ unquam fieri posse quadrata, id quod non solum valet, si a et b sint numeri inter se primi, sed etiam si compositi atque adeo fracti. Fractiones enim eiusmodi facile ad integros atque integri ad numeros inter se primos reducuntur.

COROLLARIUM 6

In his igitur duabus propositionibus evictum est sequentes novem expressiones nunquam fieri posse quadrata:

I. a^4+b^4	VI. a^4-b^4
II. a^4-4b^4	VII. $4a^4+b^4$
III. $4a^4-b^4$	VIII. $ab(aa-bb)$
IV. $ab(aa+bb)$	IX. $2ab(aa+bb)$
V. $2ab(aa-bb)$	X. $2a^4\pm 2b^4$

Decimam expressionem ideo adieci, quia eius veritas mox demonstrabitur.

THEOREMA 3

Summa duorum biquadratorum bis sumta ut $2a^4+2b^4$ *quadratum esse nequit, nisi sit* $a=b$.

DEMONSTRATIO

Pono primo a et b numeros esse inter se primos; nam nisi tales essent, formula per divisionem eo reduci posset. Facile autem perspicitur utrumque numerum a et b esse debere imparem; si enim alter par esset, tum fieret $2a^4+2b^4$ numerus impariter par, qui quadratum esse nequit. Porro haec forma congruit cum ista $(aa+bb)^2+(aa-bb)^2$, quam ideo demonstrari oportet quadratum esse non posse, nisi sit $a=b$. At ob a et b numeros impares erunt a^2+b^2 et a^2-b^2 numeri pares, ille quidem impariter, hic vero pariter par. Perventum ergo est ad hanc formam $\left(\frac{aa+bb}{2}\right)^2+\left(\frac{aa-bb}{2}\right)^2$, in qua $\frac{aa+bb}{2}$ et $\frac{aa-bb}{2}$ sint numeri inter se primi, ille impar, iste vero par; quamobrem si forma proposita esset quadratum, foret

$$\frac{aa+bb}{2}=pp-qq \quad \text{et} \quad \frac{aa-bb}{2}=2pq,$$

unde reperitur $a^2=pp+2pq-qq$ et $b^2=pp-2pq-qq$, quarum expressionum differentia est

$$4pq=aa-bb;$$

ideoque erit $a+b=\frac{2mp}{n}$ et $a-b=\frac{2nq}{m}$, unde

$$a=\frac{mp}{n}+\frac{nq}{m} \quad \text{et} \quad b=\frac{mp}{n}-\frac{nq}{m}.$$

Facta autem hac substitutione erit

$$\frac{mm}{nn}pp + \frac{nn}{mm}qq = pp - qq \quad \text{atque} \quad \frac{pp}{qq} = \frac{nn(mm+nn)}{mm(nn-mm)} = \frac{nn(n^4-m^4)}{mm(nn-mm)^2}.$$

Oporteret ergo esse quadratum $n^4 - m^4$, quod per praecedens theorema fieri nequit. Q. E. D.

COROLLARIUM 1

Si ergo a et b fuerint numeri impares, etiam $2ab(aa+bb)$ nequit esse quadratum; deberent enim a, b et $2aa+2bb$ esse quadrata, quod per hoc theorema fieri nequit.

COROLLARIUM 2

Demonstratio ergo etiam formari potuisset ex formula nona $2ab(aa+bb)$; sed ibi numerorum a et b alter positus erat par, alter impar; quod etiam si nihil impediret, tamen praestabat peculiarem dare demonstrationem.

COROLLARIUM 3

Hac igitur demonstratione ipsa formulae nonae veritas magis confirmatur, cum hinc iam constet $2ab(aa+bb)$ quadratum esse non posse, etiam si numeri a et b ambo sint impares.

COROLLARIUM 4

Brevius vero etiam veritas huius theorematis ostendi potest ex forma $(a^2+b^2)^2+(a^2-b^2)^2$, quae ideo quadratum esse nequit, quia $(a^2+b^2)^2-(a^2-b^2)^2$ est quadratum. Fieri autem nequit, ut summa duorum quadratorum sit quadratum, si eorundem quadratorum differentia fuerit quadratum. Si enim tam $pp+qq$ quam $pp-qq$ foret quadratum, quadratum esset p^4-q^4, quod fieri nequit.

COROLLARIUM 5

Simili modo $a^4 - 6aabb + b^4$ quadratum esse nequit. Est enim

$$a^4 - 6aabb + b^4 = (aa-bb)^2 - 4aabb,$$

quae est differentia eiusmodi quadratorum, quorum summa facit quadratum.

COROLLARIUM 6

Atque pari modo $a^4 + 6a^2b^2 + b^4$ quadratum esse nequit, quia est $= (a^2 + b^2)^2 + 4aabb$, quorum quadratorum summa quadratum esse nequit, quia eorundem differentia $(a^2 + b^2)^2 - 4aabb$ est quadratum.

THEOREMA 4

Duplum differentiae duorum biquadratorum ut $2a^4 - 2b^4$ quadratum esse nequit, nisi sit $a = b$.

DEMONSTRATIO

Ponamus a et b numeros inter se primos et $2a^4 - 2b^4$ esse quadratum; erunt a et b numeri impares. Foret ergo $2(a-b)(a+b)(aa+bb)$ quadratum ideoque etiam eius pars decima sexta seu $\left(\frac{a-b}{2}\right)\left(\frac{a+b}{2}\right)\left(\frac{aa+bb}{2}\right)$; qui factores cum sint inter se primi, singuli esse deberent quadrata. Sit ergo

$$\frac{a-b}{2} = pp \quad \text{et} \quad \frac{a+b}{2} = qq;$$

erit

$$a = pp + qq \quad \text{et} \quad b = qq - pp,$$

unde fit

$$\frac{aa+bb}{2} = p^4 + q^4.$$

Cum igitur $p^4 + q^4$ quadratum esse nequeat, etiam $\frac{aa+bb}{2}$ ideoque $2a^4 - 2b^4$ quadratum esse nequit. Q. E. D.

THEOREMA 5

Neque $ma^4 - m^3b^4$ neque $2ma^4 - 2m^3b^4$ potest esse quadratum.

DEMONSTRATIO

Ponamus a et b esse numeros inter se primos atque m numerum esse nec quadratum nec per quadratum divisibilem; si enim m esset divisibilis per

quadratum, tum factor quadratus per divisionem tolli posset. Ponatur porro m esse numerum tam ad a quam b primum; erunt ob

$$ma^4 - m^3b^4 = m(aa - mbb)(aa + mbb)$$

toti factores inter se primi ideoque singuli esse deberent quadrata. Facto ergo $m = pp$ deberet $(aa - ppbb)(aa + ppbb)$ esse quadratum, quod fieri nequit.

Simili modo ob $2ma^4 - 2m^3b^4 = 2m(aa - mbb)(aa + mbb)$ atque factores inter se vel primos vel binarium pro communi mensura habentes erit vel $2m$ vel m quadratum; priori vero casu facto $2m = 4pp$ oporteret esse $a^4 - 4p^4b^4$ quadratum, quod pariter fieri nequit. Sin autem $m = pp$, tum foret $2a^4 - 2p^4b^4$ quadratum, quod per theorema praecedens fieri nequit.

At si m non fuerit primus respectu ipsius a, ponamus $m = rs$ atque $a = rc$, ubi notandum est r et s numeros esse inter se primos, quia m nullum factorem quadratum habere ponitur. Quadrata ergo esse deberent istae formae $r^5sc^4 - r^3s^3b^4$ et $2r^5sc^4 - 2r^3s^3b^4$ seu $r^3sc^4 - rs^3b^4$ et $2r^3sc^4 - 2rs^3b^4$. Ob factores autem harum formularum inter se primos vel rs vel $2rs$ deberent esse quadrata adeoque r et s vel $2s$ singulatim, unde formulae orirentur, quas quadrata esse non posse iam est ostensum. Q. E. D.

COROLLARIUM 1

Huiusmodi igitur formae $mn(m^2a^4 - n^2b^4)$ et $2mn(m^2a^4 - n^2b^4)$ quadrata esse non possunt, quicunque etiam numeri loco m, n, a et b accipiantur.

COROLLARIUM 2

Si igitur $maa + nbb$ fuerit quadratum, nec $m^2naa - mn^2bb$ nec $2m^2naa - 2mn^2bb$ quadrata esse poterunt. Atque si $maa - nbb$ fuerit quadratum, nec $m^2naa + mn^2bb$ nec $2m^2naa + 2mn^2bb$ quadrata esse poterunt.

COROLLARIUM 3

Ponamus $maa + nbb = cc$; erit $m = \frac{cc - nbb}{aa}$; quadratum ergo esse neque $n(cc - nbb)(cc - 2nbb)$ neque $2n(cc - nbb)(cc - 2nbb)$ poterit. Atque si fuerit $m = \frac{cc + nbb}{aa}$, tum neutra istarum formularum $n(cc + nbb)(cc + 2nbb)$ et $2n(cc + nbb)(cc + 2nbb)$ poterit esse quadratum.

COROLLARIUM 4

Si ponatur $c = \pm pp + nqq$ et $b = 2pq$, sequentes obtinebuntur formulae $n(p^4 \pm 6nppqq + n^2q^4)$ et $2n(p^4 \pm 6nppqq + n^2q^4)$[1], quae nullo modo quadrata effici poterunt.

THEOREMA 6

Neque $ma^4 + m^3b^4$ *neque* $2ma^4 + 2m^3b^4$ *potest esse quadratum.*

DEMONSTRATIO

Dico primo, si fuerit $mp^2 - mq^2$ quadratum, tum nec $mp^2 + mq^2$ nec $2mp^2 + 2mq^2$ quadratum ullo modo esse posse; fieret enim vel $m^2(p^4 - q^4)$ vel $2m^2(p^4 - q^4)$ quadratum contra iam demonstrata. Faciamus autem $mp^2 - mq^2$ quadratum ponendo radicem eius $= \frac{(p-q)a}{b}$; erit $mp + mq = \frac{a^2p - a^2q}{bb}$, unde reperitur $q = \frac{p(aa - mbb)}{aa + mbb}$. Sit igitur $p = a^2 + mb^2$; erit $q = a^2 - mb^2$ adeoque $p^2 + q^2 = 2a^4 + 2m^2b^4$. Quadratum ergo esse non poterit primo $mp^2 + mq^2 = 2ma^4 + 2m^3b^4$, deinde $2mp^2 + 2mq^2 = 4ma^4 + 4m^3b^4$. Ex his colligitur neque $ma^4 + m^3b^4$ neque $2ma^4 + 2m^3b^4$ quadratum esse posse. Q. E. D.

COROLLARIUM

In his igitur duobus theorematis evictum est nullos numeros in istis formis $ma^4 \pm m^3b^4$ et $2ma^4 \pm 2m^3b^4$ posse esse quadratos. In his autem formulis praecedentes omnes continentur.

THEOREMA 7

FERMATIANUM[2]

Nullus numerus trigonalis in integris potest esse biquadratum praeter unitatem.

---

1) Editio princeps nec non *Commentationes arithmeticae* (ed. P. H. et N. Fuss):

$$n(p^6 \pm 6nppqq + n^2q^4) \quad et \quad 2n(p^6 \pm 6nppqq + n^2q^4).$$ Correxit F. R.

2) Hoc theorema Fermatius sine demonstratione posuerat in observationibus suis marginalibus ad *Diophantum* Bacheti primum editis a filio S. Fermatio in libro, qui inscribitur *Diophanti Alexandrini Arithmeticorum libri sex, et de numeris multangulis liber unus. Cum Commentariis C. G. Bacheti V. C. et observationibus D. P. de Fermat Senatoris Tolosani. Accessit Doctrinae Analyticae inventum novum, collectum ex variis eiusdem D. de Fermat Epistolis.* Tolosae 1670. Theorema hic tractandum invenitur in observatione ad problema XX commentarii in ultimam quaestionem *Arithmeticorum* Diophanti, p. 338; *Oeuvres de Fermat*, t. I, p. 340. F. R.

DEMONSTRATIO

Omnis numerus trigonalis hac forma $\frac{x(x+1)}{2}$ continetur. Demonstrandum ergo hanc formulam $\frac{x(x+1)}{2}$ nunquam esse posse biquadratum, siquidem loco x numeri integri substituantur excepto casu $x=1$. Notandum autem est vel x esse numerum parem vel imparem; priori igitur casu $\frac{x}{2}(x+1)$, posteriori vero $x\frac{x+1}{2}$ esse debere biquadratum; in quorum factorum utroque bini factores sunt inter se primi ideoque uterque esse deberet biquadratum. Sit igitur priori casu $\frac{x}{2}=m^4$ seu $x=2m^4$ debebitque $x+1=2m^4+1$ esse biquadratum. Posteriori vero casu sit $\frac{x+1}{2}=m^4$, ut sit $x=2m^4-1$, quod itidem oportet sit biquadratum. Hanc ob rem biquadratum esse deberet $2m^4\pm1$. Ponatur $2m^4\pm1=n^4$; erit $4m^4=2n^4\mp2$; deberet ergo $2n^4\mp2$ esse $4m^4$, hoc est quadratum. Supra autem demonstratum est $2a^4\pm2b^4$ adeoque etiam $2n^4\pm2$ nunquam quadratum esse posse praeter casum $n=1$. Posito autem $n=1$ fit m vel $=0$ vel $=1$ atque x vel $=0$ vel $=1$. Nullus igitur numerus integer datur, qui loco x substitutus redderet $\frac{x(x+1)}{2}$ biquadratum, praeter casus $x=0$ et $x=1$. Quamobrem in integris nullus extat numerus trigonalis, qui esset biquadratus, praeter unitatem et cyphram. Q. E. D.

COROLLARIUM 1

Si ponatur $\frac{xx+x}{2}=y^4$, erit $4xx+4x+1=8y^4+1=(2x+1)^2$. Ex quo sequitur numeris integris loco y substituendis hanc formam $8y^4+1$ nunquam esse posse quadratum praeter casus $y=0$ et $y=1$.

COROLLARIUM 2

Si ponatur $8y^4+1=z^2$, fiet $16y^4=2z^2-2$. Quocirca $2z^2-2$ nunquam esse potest biquadratum, quicunque numerus integer loco z substituatur, praeter casus $z=1$ et $z=3$.

THEOREMA 8

Summa trium biquadratorum, quorum duo sunt aequalia inter se, seu istiusmodi forma a^4+2b^4 quadratum esse nequit, nisi sit $b=0$.

DEMONSTRATIO

Ponamus $a^4 + 2b^4$ esse quadratum eiusque radicem $a^2 + \frac{m}{n}b^2$, ubi tam a et b quam m et n numeri erunt inter se primi. Facta autem aequatione erit $2n^2b^2 = 2mna^2 + m^2b^2$ atque

$$\frac{b^2}{a^2} = \frac{2mn}{2n^2 - m^2},$$

quae fractio vel simplicissimam iam habet formam vel divisione per 2 ad simplicissimam erit reducibilis.

Ponamus primo $2mn$ et $2n^2 - m^2$ numeros esse inter se primos, quod evenit, si m sit numerus impar, eritque

$$b^2 = 2mn \quad \text{et} \quad a^2 = 2n^2 - m^2.$$

Hic duo evolvendi sunt casus, quorum alter est, si n est numerus impar, alter, si n est par; illo casu, quo n est impar, manifestum est ob m etiam imparem $2mn$ fieri non posse quadratum, hoc vero casu, quo n est numerus par, fieri nequit $a^2 = 2n^2 - m^2$ seu $a^2 + m^2 = 2n^2$ ob a et m numeros impares et $2n^2$ numerum pariter parem.

Habeant igitur $2mn$ et $2n^2 - m^2$ communem divisorem 2, quod accidit, si m sit numerus par, puta $m = 2k$, eritque n numerus impar; habebitur ergo $\frac{b^2}{a^2} = \frac{4kn}{2n^2 - 4k^2} = \frac{2kn}{n^2 - 2k^2}$, ubi $2kn$ et $n^2 - 2k^2$ numeri erunt inter se primi. Hinc igitur ob b^2 et a^2 pariter inter se primos erit

$$b^2 = 2kn \quad \text{et} \quad a^2 = n^2 - 2k^2.$$

At hic $2kn$ fieri nequit quadratum, nisi sit k numerus par. Sit ergo k numerus par atque tam n quam $2k$ debebunt esse quadrata; fiat igitur $n = cc$ et $2k = 4dd$, ubi erit c numerus impar, hocque facto habebitur

$$a^2 = c^4 - 8d^4.$$

Quo igitur investigemus, an $c^4 - 8d^4$ possit esse quadratum, ponamus eius radicem esse $c^2 - \frac{2p}{q}d^2$ eritque $2q^2d^2 = pqc^2 - p^2d^2$ seu

$$\frac{dd}{cc} = \frac{pq}{pp + 2qq},$$

ubi iterum tam c et d quam p et q sunt numeri inter se primi. Hic denuo

duo casus sunt notandi, sive p sit numerus impar sive par. Sit ergo primo p numerus impar; habebitur ob pq et $pp+2qq$ numeros inter se primos

$$dd = pq \quad \text{et} \quad cc = pp + 2qq.$$

Necesse ergo est, ut tam p quam q sit quadratum; quamobrem pono $p = x^2$ et $q = y^2$ prodibitque

$$cc = x^4 + 2y^4;$$

quare si $a^4 + 2b^4$ esset quadratum, tum quoque foret $x^4 + 2y^4$ quadratum numerique x et y vehementer erunt minores quam a et b; ex iisque denuo minores inveniri possent, quod in integris fieri nequit. Pro secundo casu, quo p est numerus par, ponamus $p = 2r$ eritque $\frac{dd}{cc} = \frac{2qr}{2rr+2qq} = \frac{qr}{2rr+qq}$ et ob q imparem erunt qr et $2rr+qq$ numeri inter se primi. Erit ergo

$$dd = qr \quad \text{et} \quad cc = 2rr + qq,$$

quare numerorum q et r uterque debet esse quadratus; positis itaque $q = x^2$ et $r = y^2$ fiet

$$cc = 2y^4 + x^4;$$

unde patet, si $a^4 + 2b^4$ esset quadratum, tum quoque in numeris longe minoribus fore similem formam $x^4 + 2y^4$ quadratum. Quocirca $a^4 + 2b^4$ quadratum esse nequit, nisi sit $b = 0$. Q. E. D.

COROLLARIUM 1

Quoniam invenimus $\frac{b^2}{a^2} = \frac{2mn}{2n^2 - m^2}$ posito $a^4 + 2b^4$ quadrato, sequitur $2mn(2n^2 - m^2)$ quadratum esse non posse, quicunque etiam numeri loco m et n substituantur.

COROLLARIUM 2

Factis ergo $m = x^2$ et $n = y^2$ quadratum non erit haec forma $4y^4 - 2x^4$. Simili modo posito $2m = 4x^2$ et $n = y^2$ quadratum non erit haec forma $2y^4 - 4x^4$. Atque facto $m = x^2$ et $2n = 4y^2$ haec formula $8y^4 - x^4$ quadratum esse nequit.

COROLLARIUM 3

Si generaliter fiat $m = \alpha x^2$ et $n = \beta y^2$, prodibit haec formula $2\alpha\beta(2\beta^2 y^4 - \alpha^2 x^4)$ seu $4\alpha\beta^3 y^4 - 2\alpha^3\beta x^4$, quae nullo modo quadratum esse poterit.

THEOREMA 9

Si haec forma a^4+kb^4 *quadratum esse non potest, tum etiam haec forma* $2k\alpha\beta^3y^4-2\alpha^3\beta x^4$ *nullo pacto quadratum effici poterit.*

DEMONSTRATIO

Ponamus formam propositam a^4+kb^4 esse quadratum eiusque radicem $=a^2+\frac{m}{n}b^2$; erit $kn^2b^2=2mna^2+m^2b^2$ atque $\frac{b^2}{a^2}=\frac{2mn}{kn^2-m^2}$. Quia ergo a^4+kb^4 quadratum esse nequit, tum etiam $\frac{2mn}{kn^2-m^2}$ seu $2mn(kn^2-m^2)$ quadratum esse non poterit. Fiat $m=\alpha x^2$ et $n=\beta y^2$; prodibit $2\alpha\beta(k\beta^2y^4-\alpha^2x^4)$ seu $2k\alpha\beta^3y^4-2\alpha^3\beta x^4$, quae formula propterea quadratum esse non potest, quicunque numeri sive affirmativi sive negativi loco α et β substituantur. Q. E. D.

COROLLARIUM 1

Fiat sive α sive β negativum, ut prodeat haec forma $2\alpha^3\beta x^4-2k\alpha\beta^3y^4$, atque ponatur $2\alpha^3\beta=p^2$; erit $\beta=\frac{p^2}{2\alpha^3}$, unde illa forma transit in hanc $p^2x^4-\frac{kp^6}{4\alpha^8}y^4$. Quadratum ergo esse nequit haec formula x^4-4ky^4 posito $4y^4$ pro $\frac{p^4}{4\alpha^8}y^4$. Ex hac ergo formula ulterius sequitur hanc expressionem $2\alpha^3\beta x^4+8k\alpha\beta^3y^4$ quadratum fieri non posse.

COROLLARIUM 2

Ponatur in formula inventa $2k\alpha\beta^3y^4-2\alpha^3\beta x^4$ $2k\alpha\beta^3=pp$, ut sit $\alpha=\frac{pp}{2k\beta^3}$; transibit illa in hanc $p^2y^4-\frac{p^6}{4k^3\beta^8}x^4$, ex qua sequitur a^4-4kb^4 quadratum esse non posse; unde ut ante $2\alpha^3\beta x^4+8k\alpha\beta^3y^4$ quadratum esse non poterit.

COROLLARIUM 3

Si ergo a^4+kb^4 quadratum esse nequit, tum nec haec formula

$$2k\alpha\beta^3y^4-2\alpha^3\beta x^4$$

nec haec

$$\alpha^3\beta x^4+k\alpha\beta^3y^4$$

quadratum esse poterit, quae posterior ex corollariis praecedentibus sequitur scribendo 2α loco α.

COROLLARIUM 4

Cum igitur a^4+b^4 non possit esse quadratum, sequentes binae formulae $\alpha^3\beta x^4+\alpha\beta^3y^4$ et $2\alpha\beta^3y^4-2\alpha^3\beta x^4$ quadrata esse omnino non poterunt.

COROLLARIUM 5

Atque quia a^4-b^4 quadratum esse non potest, orientur hae duae novae formulae $\alpha^3\beta x^4-\alpha\beta^3y^4$ et $2\alpha^3\beta x^4+2\alpha\beta^3y^4$, quae nullo modo quadrata reddi possunt.

COROLLARIUM 6

Quoniam denique a^4+2b^4 quadratum esse nequit, istae quoque formulae $\alpha^3\beta x^4+2\alpha\beta^3y^4$ et $4\alpha\beta^3y^4-2\alpha^3\beta x^4$ non poterunt effici quadrata.

SCHOLION

Ex iis igitur, quae hactenus demonstravi, prodierunt sex sequentes formulae generaliores, quae nullo modo in quadrata transmutari possunt:

I. $\alpha^3\beta x^4+\alpha\beta^3y^4$	IV. $2\alpha^3\beta x^4-2\alpha\beta^3y^4$
II. $\alpha^3\beta x^4-\alpha\beta^3y^4$	V. $2\alpha^3\beta x^4+2\alpha\beta^3y^4$
III. $\alpha^3\beta x^4+2\alpha\beta^3y^4$	VI. $2\alpha^3\beta x^4-4\alpha\beta^3y^4$.

Atque in his sex formulis omnes continentur, quas in praecedentibus formulis tractavimus. Ex his autem formulis possent, ut iam ante feci, formulae trinomiales elici, quas aeque certum esset quadrata neutiquam reddi posse; sed iis exhibendis supersedeo ad alia nonnulla theoremata progressurus, quae circa cubos versantur atque ex istis formulis expediri nequeunt.

THEOREMA 10

Nullus cubus, ne quidem numeris fractis exceptis, unitate auctus quadratum efficere potest praeter unicum casum, quo cubus est 8.

DEMONSTRATIO

Propositio ergo huc redit, ut $\frac{a^3}{b^3}+1$ nunquam esse possit quadratum praeter casum, quo $\frac{a}{b}=2$. Quocirca demonstrandum erit hanc formulam a^3b+b^4 nunquam fieri posse quadratum, nisi sit $a=2b$.

Haec autem expressio resolvitur in istos tres factores $b(a+b)(aa-ab+bb)$, qui primo quadratum constituere possunt, si esse posset $b(a+b)=aa-ab+bb$, unde prodit $a=2b$, qui erit casus, quem excepimus. Pono autem, ut ulterius pergam, $a+b=c$ seu $a=c-b$, qua facta substitutione habebitur

$$bc(cc-3bc+3bb),$$

quam demonstrandum est quadratum esse non posse, nisi sit $c=3b$; sunt autem b et c numeri inter se primi. Hic autem duo occurrunt casus considerandi, prout c vel multiplum est ternarii vel secus; illo enim casu factores c et $cc-3bc+3bb$ communem divisorem habebunt 3, hoc vero omnes tres inter se erunt primi.

Sit primo c non divisibile per 3; necesse erit, ut singuli illi tres factores sint quadrata, scilicet b et c et $cc-3bc+3bb$ seorsim. Fiat ergo $cc-3bc+3bb=\left(\frac{m}{n}b-c\right)^2$; erit

$$\frac{b}{c}=\frac{3nn-2mn}{3nn-mm} \quad \text{vel} \quad \frac{b}{c}=\frac{2mn-3nn}{mm-3nn},$$

cuius fractionis termini erunt primi inter se, nisi m sit multiplum ternarii. Sit ergo m per 3 non divisibile; erit vel $c=3nn-mm$ vel $c=mm-3nn$ et vel $b=3nn-2mn$ vel $b=2mn-3nn$. At cum $3nn-mm$ quadratum esse nequeat, ponatur $c=mm-3nn$, quod quadratum fiat radicis $m-\frac{p}{q}n$, hincque oritur $\frac{m}{n}=\frac{3qq+pp}{2pq}$ atque

$$\frac{b}{nn}=\frac{2m}{n}-3=\frac{3qq-3pq+pp}{pq}.$$

Quadratum ergo esset haec formula $pq(3qq-3pq+pp)$, quae omnino similis est propositae $bc(3bb-3bc+cc)$ et ex multo minoribus numeris constat. At sit m multiplum ternarii, puta $m=3k$; erit $\frac{b}{c}=\frac{nn-2kn}{nn-3kk}$, unde erit vel $c=nn-3kk$ vel $c=3kk-nn$; quia autem $3kk-nn$ quadratum esse nequit, ponatur $c=nn-3kk$ eiusque radix $n-\frac{p}{q}k$, unde fiet $\frac{n}{k}=\frac{3qq+pp}{2pq}$ seu $\frac{k}{n}=\frac{2pq}{3qq+pp}$ atque

$$\frac{b}{nn}=1-\frac{2k}{n}=\frac{pp+3qq-4pq}{3qq+pp}.$$

Quadratum ergo esse deberet $(pp+3qq)(p-q)(p-3q)$. Ponatur $p-q=t$ et $p-3q=u$; erit $q=\frac{t-u}{2}$ et $p=\frac{3t-u}{2}$ illaque formula abit in hanc $tu(3tt-3tu+uu)$, quae iterum similis est priori $bc(3bb-3bc+cc)$.

Restat ergo posterior casus, quo est c multiplum ternarii, puta $c = 3d$, atque quadratum esse debet $bd(bb - 3bd + 3dd)$; quae cum iterum similis sit priori, manifestum est utroque casu evenire non posse, ut formula proposita sit quadratum. Quamobrem praeter cubum 8 alius ne in fractis quidem datur, qui cum unitate faciat quadratum. Q. E. D.

COROLLARIUM 1

Simili modo demonstrari potest nullum cubum unitate minutum esse posse quadratum; hocque ne quidem in fractis.

COROLLARIUM 2

Hinc sequitur nec $x^6 + y^6$ nec $x^6 - y^6$ esse posse quadrata atque nullum numerum trigonalem esse cubum praeter unitatem.

DE NUMERIS AMICABILIBUS[1]

Commentatio 100 indicis ENESTROEMIANI
Nova acta eruditorum 1747, p. 267—269

Problemata, quae circa indolem ac proprietates numerorum versantur, hoc tempore, quo Analysis mathematica ad multo profundiores speculationes aditum aperuit, fere penitus a Geometris derelicta videntur ac plerique arbitrantur contemplationem numerorum nihil prorsus ad augmentum Analyseos conferre. Verum tamen certe investigatio proprietatum numerorum saepenumero multo maiorem sagacitatem requirit quam subtilissimae quaestiones geometricae atque ob hanc ipsam causam quaestiones arithmeticae immerito istis postponi videntur. Ac summa quidem ingenia, quibus maxima Analyseos incrementa accepta sunt referenda, numerorum affectiones non indignas censuerunt, in quibus evolvendis plurimum operae et studii collocarent. CARTESIUM scilicet constat, etiamsi amplissimis cum universae Philosophiae tum Matheseos meditationibus esset occupatus, tamen non parum in eruendis numeris amicabilibus desudasse; quod negotium deinceps SCHOTENIUS maiori studio est persecutus. Vocantur autem numeri amicabiles duo eiusmodi numeri, quorum alter, si eius partes aliquotae omnes in unam summam colligantur, alterum producat; cuiusmodi numeri sunt 220 et 284; prioris enim 220 partes aliquotae seu divisores ipso minores

$$1+2+4+5+10+11+20+22+44+55+110$$

summam praebent 284 atque huius numeri 284 partes aliquotae

$$1+2+4+71+142$$

vicissim producunt 220. Nullum autem est dubium, quin praeter hos duos numeros plures alii atque adeo infiniti dentur, qui eadem proprietate sint

1) Vide etiam Commentationes 152 et 798 in hoc vol. 2 et in vol. 5 contentas. F. R.

praediti; neque tamen CARTESIUS et post eum SCHOOTENIUS[1]) plura quam tria talium numerorum paria elicuerunt, etiamsi non parum studii ad plura eruenda impendisse videantur. Ac methodus quidem, qua uterque est usus, ita est comparata, ut eius ope vix plures numeri amicabiles inveniri queant; assumserunt enim huiusmodi numeros in his formulis $2^n xy$ et $2^n z$ contineri, ubi x, y et z numeros primos denotent, quos ita comparatos esse oportet, ut sit primo $z = xy + x + y$, tum vero ut sit $2^n(x + y + 2) = xy + x + y + 1$. Exponenti ergo n successive varios tribuerunt valores ac pro singulis eiusmodi indagaverunt numeros primos x et y, ut posteriori aequationi satisfieret; qui si simul tales fuerint, ut $xy + x + y$ praeberet numerum primum, formulae assumtae $2^n xy$ et $2^n z$ exhibebant numeros amicabiles. Facile autem intelligitur hoc modo ad maiores exponentes n procedendo mox ad tantos numeros $xy + x + y$ perveniri, qui utrum primi sint necne, discerni amplius nequeat, cum tabula numerorum primorum ultra 100000 nondum habeatur extensa.[2])

Perspicuum autem est hanc quaestionem praeter necessitatem non leviter restringi, dum numeri amicabiles in his tantum formulis assumtis includi assumantur. Quod cum perpendissem, vocatis in subsidium nonnullis artificiis ex natura divisorum petitis plura alia numerorum amicabilium paria sum adeptus, quorum cum tribus iam notis triginta hic communicabo; eos autem, quo eorum origo et natura clarius perspiciatur, per factores expressos exhibebo. Sunt igitur numeri amicabiles:

I.	$\begin{cases} 2^2 \cdot 5 \cdot 11 \\ 2^2 \cdot 71 \end{cases}$	III.	$\begin{cases} 2^7 \cdot 191 \cdot 383 \\ 2^7 \cdot 73727 \end{cases}$
II.	$\begin{cases} 2^4 \cdot 23 \cdot 47 \\ 2^4 \cdot 1151 \end{cases}$	IV.	$\begin{cases} 2^2 \cdot 23 \cdot 5 \cdot 137 \\ 2^2 \cdot 23 \cdot 827 \end{cases}$

1) R. DESCARTES (1596—1650), *Oeuvres*, publiées par CH. ADAM et P. TANNERY, t. II, Paris 1898, p. 93—94 (Lettre CXIX de DESCARTES à MERSENNE 31 mars 1638); FR. v. SCHOOTEN (1615—1660), *Exercitationum mathematicarum libri quinque*, Lugd. Batav. 1657, lib. V sectio IX, p. 419—426. — CARTESIUS et SCHOOTENIUS haec tria paria numerorum amicabilium exposuerunt $220 = 2^2 \cdot 5 \cdot 11$ et $284 = 2^2 \cdot 71$, $17296 = 2^4 \cdot 23 \cdot 47$ et $18416 = 2^4 \cdot 1151$, $9363584 = 2^7 \cdot 191 \cdot 383$ et $9437056 = 2^7 \cdot 73727$. Quorum parium primum iam PYTHAGOREIS cognitum erat (*IAMBLICHI in NICOMACHI arithmeticam introductionem liber* ed. H. PISTELLI, Lipsiae 1894, p. 35), secundum FERMATIUS a. 1636 cum amico MERSENNE aliisque mathematicis communicaverat (P. DE FERMAT, *Varia opera mathematica*, Tolosae 1679, p. 136; *Oeuvres de FERMAT*, t. II, p. 20, 21, 71, t. IV, p. 65, 66, 67), tertium a CARTESIO a. 1638 epistola supra laudata amico MERSENNE traditum erat. F. R.

2) Vide notam 3 p. 104. F. R.

V. $\begin{cases} 3^2 \cdot 5 \cdot 13 \cdot 11 \cdot 19 \\ 3^2 \cdot 5 \cdot 13 \cdot 239 \end{cases}$

VI. $\begin{cases} 3^2 \cdot 7 \cdot 13 \cdot 5 \cdot 17 \\ 3^2 \cdot 7 \cdot 13 \cdot 107 \end{cases}$

VII. $\begin{cases} 3^2 \cdot 7^2 \cdot 13 \cdot 5 \cdot 41 \\ 3^2 \cdot 7^2 \cdot 13 \cdot 251 \end{cases}$

VIII. $\begin{cases} 2^2 \cdot 5 \cdot 131 \\ 2^2 \cdot 17 \cdot 43 \end{cases}$

IX. $\begin{cases} 2^2 \cdot 5 \cdot 251 \\ 2^2 \cdot 13 \cdot 107 \end{cases}$

X. $\begin{cases} 2^3 \cdot 17 \cdot 79 \\ 2^3 \cdot 23 \cdot 59 \end{cases}$

XI. $\begin{cases} 2^4 \cdot 23 \cdot 1367 \\ 2^4 \cdot 53 \cdot 607 \end{cases}$

XII. $\begin{cases} 2^4 \cdot 17 \cdot 10303 \\ 2^4 \cdot 167 \cdot 1103 \end{cases}$

XIII. $\begin{cases} 2^4 \cdot 19 \cdot 8563 \\ 2^4 \cdot 83 \cdot 2039 \end{cases}$ [1])

XIV. $\begin{cases} 2^4 \cdot 17 \cdot 5119 \\ 2^4 \cdot 239 \cdot 383 \end{cases}$

XV. $\begin{cases} 2^5 \cdot 59 \cdot 1103 \\ 2^5 \cdot 79 \cdot 827 \end{cases}$

XVI. $\begin{cases} 2^5 \cdot 37 \cdot 12671 \\ 2^5 \cdot 227 \cdot 2111 \end{cases}$

XVII. $\begin{cases} 2^5 \cdot 53 \cdot 10559 \\ 2^5 \cdot 79 \cdot 7127 \end{cases}$

XVIII. $\begin{cases} 2^6 \cdot 79 \cdot 11087 \\ 2^6 \cdot 383 \cdot 2309 \end{cases}$

XIX. $\begin{cases} 2^2 \cdot 11 \cdot 17 \cdot 263 \\ 2^2 \cdot 11 \cdot 43 \cdot 107 \end{cases}$

XX. $\begin{cases} 3^3 \cdot 5 \cdot 7 \cdot 71 \\ 3^3 \cdot 5 \cdot 17 \cdot 31 \end{cases}$

XXI. $\begin{cases} 3^2 \cdot 5 \cdot 13 \cdot 29 \cdot 79 \\ 3^2 \cdot 5 \cdot 13 \cdot 11 \cdot 199 \end{cases}$

XXII. $\begin{cases} 3^2 \cdot 5 \cdot 13 \cdot 19 \cdot 47 \\ 3^2 \cdot 5 \cdot 13 \cdot 29 \cdot 31 \end{cases}$

XXIII. $\begin{cases} 3^2 \cdot 5 \cdot 13 \cdot 19 \cdot 37 \cdot 1583 \\ 3^2 \cdot 5 \cdot 13 \cdot 19 \cdot 227 \cdot 263 \end{cases}$

XXIV. $\begin{cases} 3^3 \cdot 5 \cdot 31 \cdot 89 \\ 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 29 \end{cases}$

XXV. $\begin{cases} 2 \cdot 5 \cdot 7 \cdot 60659 \\ 2 \cdot 5 \cdot 23 \cdot 29 \cdot 673 \end{cases}$

XXVI. $\begin{cases} 2^3 \cdot 31 \cdot 11807 \\ 2^3 \cdot 11 \cdot 163 \cdot 191 \end{cases}$

XXVII. $\begin{cases} 3^2 \cdot 7 \cdot 13 \cdot 23 \cdot 79 \cdot 1103 \\ 3^2 \cdot 7 \cdot 13 \cdot 23 \cdot 11 \cdot 19 \cdot 367 \end{cases}$

XXVIII. $\begin{cases} 2^3 \cdot 47 \cdot 2609 \\ 2^3 \cdot 11 \cdot 59 \cdot 173 \end{cases}$

XXIX. $\begin{cases} 3^3 \cdot 5 \cdot 23 \cdot 79 \cdot 1103 \\ 3^3 \cdot 5 \cdot 23 \cdot 11 \cdot 19 \cdot 367 \end{cases}$

XXX. $\begin{cases} 3^2 \cdot 5^2 \cdot 11 \cdot 59 \cdot 179 \\ 3^2 \cdot 5^2 \cdot 17 \cdot 19 \cdot 359 \end{cases}$

---

1) Hos numeros $2^4 \cdot 19 \cdot 8563$ et $2^4 \cdot 83 \cdot 2039$ amicabiles non esse annotavit K. HUNRATH, Biblioth. Mathem. 10_3, 1909/10, p. 80. F. R.

THEOREMATA CIRCA DIVISORES NUMERORUM

Commentatio 134 indicis Enestroemiani
Novi commentarii academiae scientiarum Petropolitanae 1 (1747/8), 1750, p. 20–48
Summarium ibidem p. 35–37

SUMMARIUM

Doctissima haec dissertatio ita comparata est, ut ab harum rerum intelligentibus legi oporteat, quibus proin ieiuna quaedam recensio parum, ceteris autem lectoribus nihil commodi allaturam esse persuasi sumus. Introitus autem viri Celeberrimi in hanc dissertationem meretur, ut hic in conspectum producatur. Scilicet summos semper Geometras agnovisse asserit plurimas in natura numerorum praeclarissimas absconditas esse proprietates, quarum cognitio fines Matheseos non mediocriter esset amplificatura, tametsi iis, qui eas ad Arithmetices elementa referant, aliter visum nec creditum sit iis aliquid inesse, quod ullam sagacitatem aut vim Analyseos requirat. Hic Fermatium, insignem Geometram, testem adducit, qui diligentius in hoc genere versatus plurima huiusmodi theoremata produxit, quorum veritas evicta videtur, quamvis eius lateat demonstratio.

Sicque utique attentionem meretur, quae porro proponit in Mathesi pura, in Arithmetica scilicet, quae tamen prae reliquis Matheseos partibus maxime pertractata et perspecta haberi soleat, dari tales veritates, quas cognoscere, non autem demonstrare valeamus, cum nulla in Geometria occurrat propositio, cuius veritas sive falsitas firmissimis rationibus evinci nequeat.

Porro demonstrat in Arithmetica, ubi numerorum natura perpenditur, omnium abstrusissimas contineri veritates, quoniam veritas eo magis abstrusa censenda, quo minus ad eius demonstrationem aditus pateat.

Nec eum moratur summorum Mathematicorum auctoritas veritates huiusmodi prorsus esse steriles et haud dignas, in quarum investigatione opera collocetur, quandoque pronuntiantium. Quoniam, praeter quod omnis cognitio veritatis per se excellens sit, etiamsi

ab usu populari abhorrere videatur, etiam veritates omnes, quas nobis cognoscere licet, ita inter se esse connexas, ut nulla sine temeritate tanquam prorsus inutilis repudiari possit. Accedit, si vel maxime propositio quaedam demonstrata nihil ad utilitatem praesentem conferre videatur, quod tamen methodus, qua eius vel veritas vel falsitas eruitur, plerumque viam ad alias veritates utiliores cognoscendas patefacere soleat.

Haud ergo inutiliter operam ac studium in indagatione demonstrationum quarundam propositionum se impendisse confidit Cel. Auctor, quibus insignes circa divisores numerorum proprietates continentur.

Neque enim hanc de divisoribus doctrinam omni carere usu, sed nonnunquam in Analysi non contemnendam praestare utilitatem affirmat. Non dubitat porro Vir Cel. methodum ratiocinandi, qua usus est, in gravioribus aliis investigationibus aliquando non parum subsidii afferre posse.

Propositiones, quas hic demonstratas exhibet, divisores numerorum respiciunt in hac formula $a^n \pm b^n$ contentorum, quarum nonnullae iam ab ante memorato Fermatio, sed sine demonstratione, sunt publicatae.

De cetero omnes alphabeti litteras hic constanter numeros integros indicare monet.

Ex reliquis elegantibus meditationibus breviter notamus demonstrationem theorematis quinti sibi peculiarem esse, prouti § 20 ipse asserit Cel. Auctor.

Porro, quod § 24, 28, 31, 32 et 38 compendia quaedam insignia adducat quodque citatum § 32 problema difficillimum Fermatii, quo numerus primus dato maior quaerebatur, adhuc manere insolutum affirmet et tandem, quod veritates nonnullas, quas nosse, non autem demonstrare licet, § 59 et 69 et alias nondum ex omni parte demonstratas § 63 et 66 adducat.

Quovis tempore summi Geometrae agnoverunt in natura numerorum plurimas praeclarissimas proprietates esse absconditas, quarum cognitio fines Matheseos non mediocriter esset amplificatura. Primo quidem intuitu doctrina numerorum ad Arithmeticae elementa referenda videtur atque vix quicquam in ea inesse putatur, quod ullam sagacitatem aut vim Analyseos requirat. Qui autem diligentius in hoc genere sunt versati, non solum veritates demonstratu difficillimas detexerunt, sed etiam eiusmodi, quarum certitudo percipiatur, etiamsi demonstrari nequeat. Plurima huiusmodi theoremata sunt prolata ab insigni Geometra Fermatio, quorum veritas, quamvis demonstratio lateat, non minus evicta videtur. Atque hoc imprimis omnem attentionem meretur in Mathesi adeo pura eiusmodi dari veritates, quas nobis cognoscere liceat,

cum tamen eas demonstrare non valeamus; atque hoc adeo in Arithmetica usu venit, quae tamen prae reliquis Matheseos partibus maxime pertractata ac perspecta haberi solet; neque facile affirmare ausim, an similes veritates in reliquis partibus reperiantur. In Geometria certe nulla occurit propositio, cuius vel veritas vel falsitas firmissimis rationibus evinci nequeat. Cum igitur quaevis veritas eo magis abstrusa censeatur, quo minus ad eius demonstrationem aditus pateat, in Arithmetica certe, ubi natura numerorum perpenditur, omnium abstrusissimas contineri negare non poterimus. Non desunt quidem inter summos Mathematicos Viri, qui huiusmodi veritates prorsus steriles ideoque non dignas iudicant, in quarum investigatione ulla opera collocetur; at praeterquam quod cognitio omnis veritatis per se sit excellens, etiamsi ab usu populari abhorrere videatur, omnes veritates, quas nobis cognoscere licet, tantopere inter se connexae deprehenduntur, ut nulla sine temeritate tanquam prorsus inutilis repudiari possit. Deinde etsi quaepiam propositio ita comparata videatur, ut, sive vera sit sive falsa, nihil inde ad nostram utilitatem redundet, tamen ipsa methodus, qua eius veritas vel falsitas evincitur, plerumque nobis viam ad alias utiliores veritates cognoscendas patefacere solet.

Hanc ob rem non inutiliter me operam ac studium in indagatione demonstrationum quarundam propositionum impendisse confido, quibus insignes circa divisores numerorum proprietates continentur. Neque vero haec de divisoribus doctrina omni caret usu, sed nonnunquam in Analysi non contemnendam praestat utilitatem. Imprimis vero non dubito, quin methodus ratiocinandi, qua sum usus, in aliis gravioribus investigationibus aliquando non parum subsidii afferre possit.

Propositiones autem, quas hic demonstratas exhibeo, respiciunt divisores numerorum in hac formula $a^n \pm b^n$ contentorum, quarum nonnullae iam ab ante memorato Fermatio, sed sine demonstratione, sunt publicatae.[1]) Quoniam igitur hic perpetuo de numeris integris sermo instituetur, omnes alphabeti litterae hic constanter numeros integros indicabunt.

1) Vide Commentationem 54 huius voluminis. F. R.

THEOREMA 1

1. *Si p fuerit numerus primus, omnis numerus in hac forma $(a+b)^p - a^p - b^p$ contentus divisibilis erit per p.*

DEMONSTRATIO

Si binomium $(a+b)^p$ modo consueto evolvatur, erit

$$(a+b)^p = a^p + \frac{p}{1}a^{p-1}b + \frac{p(p-1)}{1\cdot 2}a^{p-2}b^2 + \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}a^{p-3}b^3 + \cdots$$
$$+ \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}a^3b^{p-3} + \frac{p(p-1)}{1\cdot 2}a^2b^{p-2} + \frac{p}{1}ab^{p-1} + b^p;$$

qua expressione substituta binisque terminis, qui easdem habent uncias, coniunctis erit

$$(a+b)^p - a^p - b^p = \frac{p}{1}ab(a^{p-2}+b^{p-2}) + \frac{p(p-1)}{1\cdot 2}a^2b^2(a^{p-4}+b^{p-4})$$
$$+ \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}a^3b^3(a^{p-6}+b^{p-6}) + \frac{p(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3\cdot 4}a^4b^4(a^{p-8}+b^{p-8}) + \text{etc.}$$

Hic primo notandum est omnes uncias, quamquam sub forma fractionum apparent, nihilominus esse numeros integros, cum exhibeant, uti constat, numeros figuratos. Quaelibet ergo uncia, cum factorem habeat p, divisibilis erit per p, nisi is alicubi per factorem denominatoris vel prorsus tollatur vel dividatur. At ubique omnes factores denominatorum minores sunt quam p, quia adeo non ultra $\frac{1}{2}p$ crescunt, ideoque factor numeratorum p nusquam per divisionem tollitur. Deinde cum p sit per hypothesin numerus primus, is nusquam per divisionem minuetur. Quocirca singulae unciae $\frac{p}{1}$, $\frac{p(p-1)}{1\cdot 2}$, $\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}$ etc. hincque tota expressio $(a+b)^p - a^p - b^p$ perpetuo per numerum p, siquidem fuerit numerus primus, erit divisibilis. Q. E. D.

COROLLARIUM 1

2. Si ergo ponatur $a=1$ et $b=1$, erit $2^p - 2$ semper divisibilis per p, si quidem fuerit p numerus primus. Cum igitur sit $2^p - 2 = 2(2^{p-1}-1)$,

alterum horum factorum per p divisibilem esse oportet. At nisi sit $p = 2$, prior factor 2 per p non est divisibilis; unde sequitur formam $2^{p-1} - 1$ perpetuo per p esse divisibilem, si p fuerit numerus primus praeter binarium.

COROLLARIUM 2

3. Ponendis ergo pro p successive numeris primis erit $2^2 - 1$ divisibile per 3, $2^4 - 1$ per 5, $2^6 - 1$ per 7, $2^{10} - 1$ per 11 etc., quod in minoribus numeris per se fit perspicuum, in maximis autem aeque erit certum. Sic cum 641 sit numerus primus, iste numerus $2^{640} - 1$ necessario per 641 erit divisibilis, seu si potestas 2^{640} per 641 dividatur, post divisionem supererit residuum $= 1$.

THEOREMA 2

4. *Si utraque harum formularum* $a^p - a$ et $b^p - b$ *fuerit divisibilis per numerum primum* p, *tum quoque ista formula* $(a + b)^p - a - b$ *divisibilis erit per eundem numerum primum* p.

DEMONSTRATIO

Cum per § 1 $(a + b)^p - a^p - b^p$ sit divisibilis per numerum p, si fuerit primus, atque hic formulae $a^p - a$ et $b^p - b$ per p divisibiles assumantur, erit quoque summa istarum trium formularum, nempe $(a + b)^p - a - b$, per p, si fuerit numerus primus, divisibilis. Q. E. D.

COROLLARIUM 1

5. Si ponatur $b = 1$, cum $1^p - 1 = 0$ sit divisibile per p, sequitur, si formula $a^p - a$ fuerit divisibilis per p, tum quoque formulam $(a + 1)^p - a - 1$ fore per p divisibilem.

COROLLARIUM 2

6. Cum igitur assumta formula $a^p - a$ per p divisibili sit quoque formula $(a + 1)^p - a - 1$ per p divisibilis, simili modo in eadem hypothesi erit haec quoque formula $(a + 2)^p - a - 2$ hincque porro haec $(a + 3)^p - a - 3$ etc. atque generaliter haec $c^p - c$ divisibilis per p.

THEOREMA 3

7. *Si p fuerit numerus primus, omnis numerus huius formae $c^p - c$ per p erit divisibilis.*

DEMONSTRATIO

Si in § 6 ponatur $a = 1$, cum sit $a^p - a = 0$ per p divisibilis, sequitur has quoque formulas $2^p - 2$, $3^p - 3$, $4^p - 4$ etc. et generatim hanc $c^p - c$ fore per numerum primum p divisibilem. Q. E. D.

COROLLARIUM 1

8. Quicunque ergo numerus integer pro c assumatur, denotante p numerum primum omnes numeri in hac forma $c^p - c$ contenti erunt divisibiles per p.

COROLLARIUM 2

9. Cum autem sit $c^p - c = c(c^{p-1} - 1)$, vel ipse numerus c vel $c^{p-1} - 1$ divisibilis erit per p. Utrumque autem simul per p divisibilem esse non posse manifestum est. Quare si numerus c non fuerit divisibilis per p, haec forma $c^{p-1} - 1$ certe per p erit divisibilis.

COROLLARIUM 3

10. Si ergo p fuerit numerus primus, omnes numeri in hac forma contenti $a^{p-1} - 1$ erunt divisibiles per p exceptis iis casibus, quibus ipse numerus a per p est divisibilis.[1])

THEOREMA 4

11. *Si neuter numerorum a et b divisibilis fuerit per numerum primum p, tum omnis numerus huius formae $a^{p-1} - b^{p-1}$ erit divisibilis per p.*

DEMONSTRATIO

Cum neque a neque b sit divisibilis per p atque p denotet numerum primum, tam haec forma $a^{p-1} - 1$ quam haec $b^{p-1} - 1$ erit divisibilis per p. Hinc ergo quoque differentia istarum formularum $a^{p-1} - b^{p-1}$ erit divisibilis per p. Q. E. D.

---

1) Aliae huius theorematis FERMATIANI demonstrationes inveniuntur in Commentationibus 54 et 262 (§ 49) huius voluminis. Vide etiam notam 2 p. 34. F. R.

COROLLARIUM 1

12. Cum omnis numerus primus praeter binarium, cuius ratio dividendi per se est manifesta, sit impar, ponatur $2m+1$ pro p atque perspicuum erit omnes numeros in hac forma $a^{2m}-b^{2m}$ contentos esse divisibiles per $p=2m+1$, siquidem neque a neque b seorsim fuerit per $2m+1$ divisibilis.

COROLLARIUM 2

13. Quia b non est divisibilis per $2m+1$, etiam b^{2m} et $2b^{2m}$ non divisibile erit per $2m+1$. Quare si $2b^{2m}$ addatur ad formulam $a^{2m}-b^{2m}$, quae est divisibilis per $2m+1$, prodibit formula $a^{2m}+b^{2m}$, quae per $2m+1$ non erit divisibilis, nisi uterque numerus a et b seorsim per $2m+1$ sit divisibilis.

COROLLARIUM 3

14. Quoniam ob $2m$ numerum parem formula $a^{2m}-b^{2m}$ factores habet $(a^m-b^m)(a^m+b^m)$, necesse est, ut horum factorum alter sit divisibilis per $2m+1$; ambo autem simul per numerum $2m+1$ divisibiles esse nequeunt. Quare si $2m+1$ fuerit numerus primus et neque a neque b divisibile sit per $2m+1$, tum vel a^m-b^m vel a^m+b^m erit divisibile per $2m+1$.

COROLLARIUM 4

15. Si m sit numerus par, puta $=2n$, atque a^m-b^m seu $a^{2n}-b^{2n}$ divisibilis per $2m+1=4n+1$, tum ob eandem rationem vel a^n-b^n vel a^n+b^n divišibile erit per numerum primum $4n+1$.

THEOREMA 5

16. *Summa duorum quadratorum* $aa+bb$ *per nullum numerum primum huius formae* $4n-1$ *unquam dividi potest, nisi utriusque radix seorsim* a *et* b *sit divisibilis per* $4n-1$.

DEMONSTRATIO

Si $4n-1$ fuerit numerus primus neque a et b per illum sint divisibiles, tum $a^{4n-2}-b^{4n-2}$ erit divisibile per $4n-1$ (§ 11) hincque ista formula $a^{4n-2}+b^{4n-2}$ non erit divisibilis per $4n-1$ [§ 13] neque propterea ullus eius

factor. At cum $4n-2=2(2n-1)$ sit numerus impariter par, formula $a^{4n-2}+b^{4n-2}$ factorem habet $aa+bb$; quare fieri nequit, ut iste factor $aa+bb$, hoc est ulla duorum quadratorum summa, sit divisibilis per $4n-1$. Q. E. D.[1])

COROLLARIUM 1

17. Cum omnes numeri primi vel ad hanc formam $4n+1$ vel ad hanc $4n-1$ revocentur, si $4n-1$ non fuerit numerus primus, divisorem habebit formae $4n-1$; namque ex meris numeris formae $4n+1$ nunquam numerus formae $4n-1$ resultare potest. Quare cum summa duorum quadratorum per nullum numerum primum formae $4n-1$ dividi possit, per nullum quoque numerum eiusdem formae $4n-1$, etiamsi non sit primus, dividi poterit.

COROLLARIUM 2

18. Summa ergo duorum quadratorum $aa+bb$ per nullum numerum huius seriei

$$3,\ 7,\ 11,\ 15,\ 19,\ 23,\ 27,\ 31,\ 35 \text{ etc.}$$

est divisibilis. Omnes ergo numeri primi praeter binarium, qui unquam divisores esse possunt summae duorum quadratorum, continentur in hac forma $4n+1$, siquidem numeri a et b inter se communem divisorem non habent.

COROLLARIUM 3

19. Cum omnis numerus sit vel primus vel productum ex primis, summa duorum quadratorum nullum numerum primum pro divisore habebit, nisi qui contineatur in hac forma $4n+1$. Divisores ergo primi summae duorum quadratorum continebuntur in hac serie

$$2,\ 5,\ 13,\ 17,\ 29,\ 37,\ 41,\ 53,\ 61,\ 73,\ 89,\ 97 \text{ etc.}$$

SCHOLION

20. Quod numerus huius formae $4n-1$ nunquam possit esse summa duorum quadratorum, facile intelligitur. Numeri enim quadrati vel sunt pares vel impares; illi in hac forma $4a$, hi vero in hac $4b+1$ continentur.

1) Alia huius theorematis demonstratio invenitur in Commentatione 242 (§ 70) huius voluminis. F. R.

Quare ut summa duorum quadratorum sit numerus impar, alterum par, alterum impar esse oportet; hinc oritur forma $4a+4b+1$ seu $4n+1$ ideoque nullus numerus huius formae $4n-1$ summa duorum quadratorum esse potest. Quod vero summa duorum quadratorum ne divisorem quidem formae $4n-1$ admittat, ab omnibus scriptoribus methodi DIOPHANTEAE semper est affirmatum; nemo autem unquam, quantum mihi constat, id demonstravit excepto FERMATIO[1]), qui autem suam demonstrationem nunquam publicavit, ita ut mihi quidem videar primus hanc veritatem publice demonstrasse: *Nullum numerum vel huius formae* $4n-1$ *vel per numerum eiusdem formae divisibilem unquam esse posse summam duorum quadratorum.* Hinc ergo sequitur omnem summam duorum quadratorum inter se primorum vel esse numerum primum vel binario excepto alios divisores non habere, nisi qui in forma $4n+1$ contineantur.

THEOREMA 6

21. *Omnes divisores summae duorum biquadratorum inter se primorum sunt vel 2 vel numeri huius formae* $8n+1$.

DEMONSTRATIO

Sint a^4 et b^4 duo biquadrata inter se prima; erit vel utrumque impar vel alterum par et alterum impar; priori casu summae a^4+b^4 divisor erit 2, utroque vero casu divisores impares, si qui fuerint, in hac forma $4n+1$ continebuntur. Cum enim biquadrata simul sint quadrata, nullus divisor formae $4n-1$ locum invenit (§ 16). At numeri $4n+1$ vel ad hanc formam $8n+1$ vel ad hanc $8n-3$ revocantur. Dico autem nullum numerum formae

1) P. DE FERMAT, *Varia opera mathematica*, Tolosae 1679, p. 161 (Lettre de FERMAT à ROBERVAL [août 1640]); *Oeuvres de* FERMAT, t. II, p. 202. Verisimile est iam DIOPHANTUM theorema hic tractatum cognosse. Vide quaestionem XII libri V DIOPHANTI *Arithmeticorum* (*Opera omnia* ed. P. TANNERY, vol. I, Lipsiae 1893, p. 332; *Die Arithmetik und die Schrift über Polygonalzahlen des* DIOPHANTUS *von Alexandria.* Übersetzt und mit Anmerkungen begleitet von G. WERTHEIM, Leipzig 1890, p. 206) nec non FERMATII observationes ad commentarium BACHETI in hanc quaestionem, p. 214 et 225 editionis supra (nota 2 p. 51 huius voluminis) commemoratae; *Oeuvres de* FERMAT, t. I, p. 312 et 313. Vide etiam F. CAJORI, *On* MICHEL ROLLE'*s book „Methode pour résoudre les egalitez“ and the history of „*ROLLE'*s theorem“* Biblioth. Mathem. 11_3, 1910/11, p. 300, imprimis p. 311—313. F. R.

$8n-3$ esse posse divisorem summae duorum biquadratorum. Ad hoc demonstrandum sit primo $8n-3$ numerus primus atque per eum divisibilis erit haec forma $a^{8n-4}-b^{8n-4}$, unde haec forma $a^{8n-4}+b^{8n-4}$ per numerum $8n-3$ prorsus non erit divisibilis [§ 13], nisi uterque numerus a et b seorsim divisionem admittat, qui casus autem assumtione, quod ambo numeri a et b sint inter se primi, excluditur. Cum igitur forma $a^{8n-4}+b^{8n-4}=a^{4(2n-1)}+b^{4(2n-1)}$ dividi nequeat per $8n-3$, nullus quoque eius factor per $8n-3$ dividi poterit. At ob $2n-1$ numerum imparem illius formae factor erit a^4+b^4, qui ergo per nullum numerum primum formae $8n-3$ dividi potest. Hinc omnes numeri primi praeter binarium, qui unquam formam a^4+b^4 divident, erunt huiusmodi $8n+1$. Ex multiplicatione autem duorum pluriumve talium divisorum nunquam numerus formae $8n-3$ oritur; ex quo sequitur nullum prorsus numerum huius formae $8n-3$, sive sit primus sive compositus, summam duorum biquadratorum inter se primorum dividere. Q. E. D.

COROLLARIUM 1

22. Cum omnes numeri impares in una harum quatuor formarum contineantur $8n\pm1$ et $8n\pm3$, praeter numeros in forma prima $8n+1$ contentos nullus alius poterit esse divisor summae duorum biquadratorum.

COROLLARIUM 2

23. Omnes ergo divisores primi summae duorum biquadratorum inter se primorum erunt vel 2 vel in hac serie contenti

$$17,\ 41,\ 73,\ 89,\ 97,\ 113,\ 137,\ 193 \text{ etc.},$$

quae complectitur omnes numeros primos formae $8n+1$.

COROLLARIUM 3

24. Si quis ergo numerus, puta N, fuerit summa duorum biquadratorum, tum is vel erit primus vel alios non habebit divisores, nisi qui in forma $8n+1$ contineantur; unde investigatio divisorum mirum in modum contrahitur.

COROLLARIUM 4

25. Nullus igitur numerus, qui divisorem habet non in forma $8n+1$ contentum, erit summa duorum biquadratorum, nisi forte habeat quatuor divisores aequales, qui autem in consideratione biquadratorum reiici solent.

THEOREMA 7

26. *Omnes divisores huiusmodi numerorum* a^8+b^8, *si quidem a et b sunt numeri inter se primi, sunt vel* 2 *vel in hac forma* $16n+1$ *continentur.*

DEMONSTRATIO

Quia a^8 et b^8 simul sunt biquadrata, eorum summa a^8+b^8 alios non admittet divisores, nisi qui in forma $8n+1$ contineantur. At numeri in hac forma $8n+1$ contenti sunt vel $16n+1$ vel $16n-7$. Sit $16n-7$ numerus primus ac per eum dividi non poterit forma $a^{16n-8}+b^{16n-8}$ (§ 13) seu $a^{8(2n-1)}+b^{8(2n-1)}$ neque propterea ullus eius factor. Verum ob $2n-1$ numerum imparem haec forma divisorem habet a^8+b^8, quae ergo per nullum numerum primum $16n-7$ erit divisibilis ac propterea alios divisores primos habere nequit, nisi qui in forma $16n+1$ contineantur. Ex multiplicatione autem duorum pluriumve huiusmodi numerorum $16n+1$ perpetuo productum eiusdem formae nascitur neque unquam numerus formae $16n-7$ resultare potest. Unde cum nullus numerus formae $16n-7$ divisor ipsius a^8+b^8 existere possit, necesse est, ut omnes huius formae a^8+b^8 divisores, si quos habet, sive sint primi sive compositi, perpetuo in hac formula $16n+1$ contineantur. Q. E. D.

COROLLARIUM 1

27. Nullus igitur numerus, qui in hac forma $16n+1$ non includitur, unquam esse potest divisor summae duarum potestatum octavi gradus inter se primarum.

COROLLARIUM 2

28. Si quis ergo voluerit numeri cuiuspiam huius formae a^8+b^8 divisores investigare, is divisionem per nullos alios numeros primos nisi in hac forma $16n+1$ contentos tentet, cum demonstratum sit omnes reliquos numeros primos huius formae divisores esse non posse.

THEOREMA 8

29. *Summa duarum huiusmodi potestatum $a^{2^m}+b^{2^m}$, quarum exponens est dignitas binarii, alios divisores non admittit, nisi qui contineantur in hac forma $2^{m+1}n+1$.*

DEMONSTRATIO

Quemadmodum demonstravimus omnes divisores formae a^2+b^2 in hac forma $4n+1$ contineri hincque ulterius divisores omnes formae a^4+b^4 in $8n+1$ et formae a^8+b^8 in $16n+1$ contineri evicimus, ita simili modo ostendi potest formam $a^{16}+b^{16}$ nullos alios divisores admittere nisi in formula $32n+1$ contentos. Dehinc porro intelligemus formas $a^{32}+b^{32}$, $a^{64}+b^{64}$ etc. alios divisores habere non posse, nisi qui in formulis $64n+1$, $128n+1$ etc. includantur. Sicque in genere patebit formae $a^{2^m}+b^{2^m}$ alios non dari divisores, nisi qui in formula $2^{m+1}n+1$ contineantur. Q. E. D.

COROLLARIUM 1

30. Nullus ergo numerus primus, qui in hac forma $2^{m+1}n+1$ non includitur, unquam esse potest divisor ullius numeri in hac forma $a^{2^m}+b^{2^m}$ contenti.

COROLLARIUM 2

31. Divisores ergo huiusmodi numeri $a^{2^m}+b^{2^m}$ inquisiturus inutiliter operam suam consumeret, si aliis numeris primis praeter eos, quos forma $2^{m+1}n+1$ suppeditat, divisionem tentare vellet.

SCHOLION 1

32. FERMATIUS affirmaverat, etiamsi id se demonstrare non posse ingenue esset confessus, omnes numeros ex hac forma $2^{2^m}+1$ ortos esse primos[1]; hincque problema alias difficillimum, quo quaerebatur numerus primus dato numero maior, resolvere est conatus. Ex ultimo theoremate autem perspicuum est, nisi numerus $2^{2^m}+1$ sit primus, eum alios divisores habere non

1) Vide Commentationem 26 huius voluminis. F. R.

posse praeter tales, qui in forma $2^{m+1}n+1$ contineantur. Cum igitur veritatem huius effati FERMATIANI pro casu $2^{32}+1$ examinare voluissem, ingens hinc compendium sum nactus, dum divisionem aliis numeris primis praeter eos, quos formula $64n+1$ suppeditat, tentare non opus habebam. Huc igitur inquisitione reducta mox deprehendi ponendo $n=10$ numerum primum 641 esse divisorem numeri $2^{32}+1$, unde problema memoratum, quo numerus primus dato numero maior requiritur, etiamnum manet insolutum.

SCHOLION 2

33. Summa duarum potestatum eiusdem gradus, uti a^m+b^m, semper habet divisores algebraice assignabiles, nisi m sit dignitas binarii. Nam si m sit numerus impar, tum a^m+b^m semper divisorem habet $a+b$, atque si p fuerit divisor ipsius m, tum quoque a^p+b^p formam a^m+b^m dividet. Sin autem m sit numerus par, in hac formula $2^n p$ continebitur, ita ut p sit numerus impar, hocque casu $a^{2^n}+b^{2^n}$ divisor erit formae a^m+b^m existente $m=2^n p$. Atque si p habeat divisorem q, tum etiam $a^{2^n q}+b^{2^n q}$ erit divisor formae a^m+b^m. Quocirca a^m+b^m numerus primus esse nequit, nisi m sit dignitas binarii. Hoc igitur casu, si a^m+b^m non fuerit numerus primus, alios divisores habere nequit, nisi qui formula $2mn+1$ contineantur.

Contra autem si differentia duarum potestatum eiusdem gradus proponatur a^m-b^m, ea semper divisorem habet $a-b$; praeterea vero si exponens m divisorem habeat p, erit quoque a^p-b^p divisor formae a^m-b^m. Hinc si m sit numerus primus, forma a^m-b^m praeter $a-b$ alium divisorem algebraice assignabilem non habebit; quare si a^m-b^m fuerit numerus primus, necesse est, ut m sit numerus primus et $a-b=1$. Interim tamen ne his quidem casibus forma a^m-b^m semper est numerus primus, sed quoties $2m+1$ est numerus primus, per eum erit divisibilis. Praeterea vero etiam alios divisores habere potest, quos hic sum investigaturus.

THEOREMA 9

34. *Si differentia potestatum a^m-b^m fuerit divisibilis per numerum primum $2n+1$ atque p sit maximus communis divisor numerorum m et $2n$, tum quoque a^p-b^p erit divisibilis per $2n+1$.*

DEMONSTRATIO

Quia $2n+1$ est numerus primus, erit $a^{2n}-b^{2n}$ divisibilis per $2n+1$, et cum per hypothesin a^m-b^m sit quoque divisibilis per $2n+1$, sit $2n=\alpha m+q$ seu q sit residuum in divisione ipsius $2n$ per m remanens; et cum $a^{\alpha m}-b^{\alpha m}$ sit quoque per $2n+1$ divisibilis, multiplicetur haec forma per a^q; erit $a^{\alpha m+q}-a^q b^{\alpha m}$ per $2n+1$ divisibilis; at posito $\alpha m+q$ pro $2n$ est quoque $a^{\alpha m+q}-b^{\alpha m+q}$ per $2n+1$ divisibilis; a qua formula si prior subtrahatur, residuum $a^q b^{\alpha m}-b^{\alpha m+q}=b^{\alpha m}(a^q-b^q)$ quoque per $2n+1$ erit divisibile. Hinc cum b per hypothesin divisorem $2n+1$ non habeat, necesse est, ut a^q-b^q per $2n+1$ sit divisibile. Ponatur porro $m=\beta q+r$, et cum utraque haec formula $a^{\beta q+r}-b^{\beta q+r}$ et $a^{\beta q}-b^{\beta q}$ sit per $2n+1$ divisibilis, multiplicetur posterior per a^r et a priori subtrahatur atque residuum $b^{\beta q}(a^r-b^r)$ seu a^r-b^r pariter per $2n+1$ erit divisibile. Simili modo patebit, si fuerit $q=\gamma r+s$, tum formulam a^s-b^s per $2n+1$ fore divisibilem; atque si per huiusmodi continuam divisionem valores litterarum q, r, s, t etc. investigentur, tandem pervenietur ad maximum communem divisorem numerorum m et $2n$; qui ergo si ponatur $=p$, erit a^p-b^p divisibile per $2n+1$. Q. E. D.

COROLLARIUM 1

35. Si igitur m fuerit numerus ad $2n$ primus, maximus eorum communis divisor erit unitas, ac propterea si a^m-b^m fuerit divisibile per numerum primum $2n+1$, tum quoque $a-b$ per $2n+1$ erit divisibile.

COROLLARIUM 2

36. Si ergo differentia numerorum $a-b$ non fuerit divisibilis per $2n+1$, tum quoque nulla huiusmodi forma a^m-b^m, ubi m est ad $2n$ numerus primus, per $2n+1$ divisibilis esse potest.

COROLLARIUM 3

37. Quodsi ergo m fuerit numerus primus, forma a^m-b^m per numerum primum $2n+1$ dividi non potest, nisi m sit divisor ipsius $2n$, posito quod $a-b$ non sit divisibile per $2n+1$.

COROLLARIUM 4

38. Existente ergo m numero primo haec forma $a^m - b^m$ praeter divisorem $a-b$ alios divisores habere nequit, nisi qui includantur in hac formula $mn+1$. Unde divisores numeri cuiuspiam in hac forma $a^m - b^m$ contenti investigaturus divisionem tantum per numeros primos in forma $mn+1$ contentos tentabit.

COROLLARIUM 5

39. Nisi ergo numerus $2^m - 1$ sit primus existente m numero primo, alios divisores habere non poterit, nisi qui includantur in hac forma $mn+1$.

COROLLARIUM 6

40. Si ergo m sit numerus primus, divisores formulae $a^m - b^m$ praeter $a-b$, si quidem a et b fuerint numeri inter se primi, continebuntur in hac serie

$$2m+1, \quad 4m+1, \quad 6m+1, \quad 8m+1, \quad 10m+1 \quad \text{etc.},$$

si hinc numeri non primi expungantur.

THEOREMA 10

41. *Si formula $a^m \pm b^m$ divisorem habeat p, tum quoque haec expressio $(a \pm \alpha p)^m \pm (b \pm \beta p)^m$ per p erit divisibilis.*

DEMONSTRATIO

Si potestates $(a \pm \alpha p)^m$ et $(b \pm \beta p)^m$ methodo consueta evolvantur, in utraque serie omnes termini praeter primum divisibiles erunt per p. Scilicet formula $(a \pm \alpha p)^m \pm (b \pm \beta p)^m$ abibit in hanc formam

$$+\ a^m \pm m a^{m-1} \alpha p + \frac{m(m-1)}{1 \cdot 2} a^{m-2} \alpha^2 p^2 \pm \text{etc.}$$

$$\pm (b^m \pm m b^{m-1} \beta p + \frac{m(m-1)}{1 \cdot 2} b^{m-2} \beta^2 p^2 \pm \text{etc.}).$$

Unde perspicuum est: si $a^m \pm b^m$ fuerit divisibile, tum quoque haec forma $(a \pm \alpha p)^m \pm (b \pm \beta p)^m$ per p erit divisibilis. Q. E. D.

COROLLARIUM 1

42. Si igitur $a^m \pm 1$ fuerit divisibile per p, tum quoque haec formula $(a \pm \alpha p)^m \pm 1$ per p erit divisibilis.

COROLLARIUM 2

43. Si $a^m \pm b^m$ fuerit divisibile per p, tum quoque haec formula $(a \pm \alpha p)^m \pm b^m$ vel haec $a^m \pm (b \pm \beta p)^m$ per p erit divisibilis.

SCHOLION

44. Eodem quoque modo generaliter demonstrari potest, si fuerit $Aa^m \pm Bb^m$ divisibile per p, tum quoque hanc formam $A(a \pm \alpha p)^m \pm B(b \pm \beta p)^m$ fore per p divisibilem. Haecque veritas aeque locum invenit, sive p sit numerus primus sive secus. Quin etiam non opus est, ut utriusque potestatis idem sit exponens m, sed etiamsi essent inaequales, conclusio perinde valebit. Tum vero quoque, si m fuerit numerus par, ex divisibilitate formulae $a^m \pm b^m$ per numerum p divisibilitas etiam huius formulae $(\alpha p \pm a)^m \pm (\beta p \pm b)^m$ sequitur. Verum haec aliaque similia ex algebrae elementis sponte patent.

THEOREMA 11

45. *Si fuerit* $a = ff \pm (2m+1)\alpha$ *et* $2m+1$ *numerus primus, tum ista expressio* $a^m - 1$ *erit divisibilis per* $2m+1$.

DEMONSTRATIO

Cum sit $2m+1$ numerus primus, per eum dividi poterit haec formula $f^{2m} - 1$ seu haec $(ff)^m - 1$. Hinc per theorema praecedens quoque ista formula $(ff \pm (2m+1)\alpha)^m - 1$ erit divisibilis per $2m+1$. Quare si fuerit $a = ff \pm (2m+1)\alpha$, formula $a^m - 1$ per numerum primum $2m+1$ dividi poterit. Q. E. D.

COROLLARIUM 1

46. Si ergo fuerit vel $a = (2m+1)\alpha + 1$ vel $a = (2m+1)\alpha + 4$ vel $a = (2m+1)\alpha + 9$ vel $a = (2m+1)\alpha + 16$ vel etc., tum formula $a^m - 1$ semper erit divisibilis per $2m+1$, si quidem $2m+1$ fuerit numerus primus.

COROLLARIUM 2

46[a][1]). Cum casus, quibus ipse numerus a est divisibilis per $2m+1$ excludantur, manifestum est in formula $ff+(2m+1)a$ numerum f per $2m+1$ divisibilem esse non posse. Hinc pro f omnes numeri assumi possunt, qui per $2m+1$ non sint divisibiles.

COROLLARIUM 3

47. Numeri ergo pro f assumendi sunt

$$(2m+1)k\pm 1,\quad (2m+1)k\pm 2,\quad (2m+1)k\pm 3,\quad \ldots\quad (2m+1)k\pm m;$$

in his enim formulis omnes numeri per $2m+1$ non divisibiles continentur. Hinc sumendis quadratis formae ipsius a, si quidem partes per $2m+1$ divisibiles in unam colligantur, erunt sequentes

$$(2m+1)p+1,\quad (2m+1)p+4,\quad (2m+1)p+9,\quad \ldots\quad (2m+1)p+mm,$$

quarum numerus est m.

COROLLARIUM 4

48. Ad valores igitur ipsius a inveniendos, ut a^m-1 per numerum $2m+1$ fiat divisibile, investigari oportet residua, quae in divisione cuiusque numeri quadrati per $2m+1$ remanent. Si enim r fuerit huiusmodi residuum, erit $(2m+1)p+r$ idoneus valor pro a.

COROLLARIUM 5

49. Omnia haec residua r erunt autem minora quam $2m+1$, neque tamen omnes numeri minores quam $2m+1$ erunt valores ipsius r, quia numerus valorum ipsius r maior esse nequit quam m. Dabuntur ergo semper m numeri, qui pro r adhiberi non poterunt.

COROLLARIUM 6

50. Valores vero ipsius r erunt primo omnes numeri quadrati ipso $2m+1$ minores, tum vero residua, quae in divisione maiorum quadratorum

1) In editione principe falso numerus 46 iteratur. F. R.

per $2m+1$ remanent; neque tamen unquam numerus omnium diversorum valorum ipsius r maior esse poterit numero m.

SCHOLION

51. Ut usus huius theorematis clarius appareat atque per exempla numerica illustrari possit, sequentia problemata adiicere visum est, ex quibus non solum veritas theorematis luculentius perspicietur, sed etiam vicissim patebit, quoties a non habuerit valorem hic assignatum, toties formulam a^m-1 non esse divisibilem per $2m+1$. Cum igitur haec formula $a^{2m}-1$ semper sit divisibilis per $2m+1$, quoties a^m-1 divisionem per $2m+1$ non admittit, toties a^m+1 per $2m+1$ divisibile esse oportebit.

EXEMPLUM 1

52. *Invenire valores ipsius a, ut a^2-1 fiat divisibile per* 5.

Residua, quae ex divisione quadratorum per 5 remanent, sunt 1 et 4; hinc necesse est, ut sit vel $a=5p+1$ vel $a=5p+4$ sive $a=5p-1$. Priori casu fit $aa-1$ seu $(a-1)(a+1)=5p(5p+2)$, posteriori autem $=(5p-2)5p$; utroque ergo divisibilitas per 5 perspicitur. Sin autem fuerit vel $a=5p+2$ vel $a=5p+3$, neutro casu formula $aa-1$ per 5 erit divisibilis.

EXEMPLUM 2

53. *Invenire valores ipsius a, ut haec forma a^3-1 fiat per* 7 *divisibilis.*

Tria residua, quae in divisione omnium quadratorum per 7 remanent, sunt 1, 2, 4. Hinc valores ipsius a sunt $7p+1$, $7p+2$ et $7p+4$; sin autem fuerit vel $a=7p+3$ vel $7p+5$ vel $7p+6$, tum non formula proposita a^3-1, sed haec a^3+1 per 7 fiet divisibilis.

EXEMPLUM 3

54. *Invenire valores ipsius a, ut haec forma a^5-1 fiat per* 11 *divisibilis.*

Numeri quadrati per 11 divisi dabunt 5 diversa residua, quae sunt 1, 3, 4, 5, 9. Hinc formula a^5-1 per 11 erit divisibilis, si fuerit $a=11p+r$

denotante r unumquemque ex numeris 1, 3, 4, 5, 9. Sin autem pro a sumatur quidam ex his numeris 2, 6, 7, 8, 10 multiplo quocunque ipsius 11 auctus, tum $a^5 + 1$ per 11 erit divisibile.

THEOREMA 12

55. *Si fuerit* $a = f^3 \pm (3m+1)\alpha$ *existente* $3m+1$ *numero primo, tum haec forma* $a^m - 1$ *semper erit per* $3m+1$ *divisibilis.*

DEMONSTRATIO

Ob $3m+1$ numerum primum erit $f^{3m} - 1$ divisibile per $3m+1$. At est $f^{3m} - 1 = (f^3)^m - 1$, unde quoque haec formula $(f^3 \pm (3m+1)\alpha)^m - 1$ erit divisibilis per $3m+1$. Quare si sumatur $a = f^3 \pm (3m+1)\alpha$, tum haec formula $a^m - 1$ erit per $3m+1$ divisibilis. Q. E. D.

COROLLARIUM 1

56. Ad valores ergo ipsius a inveniendos omnia residua, quae oriuntur, si cubi per $3m+1$ dividantur, notari debent. Unumquodque enim horum residuorum multiplo ipsius $3m+1$ quocunque auctum dabit valorem idoneum pro a.

COROLLARIUM 2

57. Cum $3m+1$ esse debeat numerus primus, necesse est, ut m sit numerus par, sicque numerus primus $3m+1$ unitate superabit multiplum senarii. Hinc erunt numeri pro m et $3m+1$ adhibendi sequentes:

$$m = 2,\ 4,\ 6,\ 10,\ 12,\ 14,\ 20,\ 22,\ 24,\ 26,\ 32 \text{ etc.},$$

$$3m+1 = 7,\ 13,\ 19,\ 31,\ 37,\ 43,\ 61,\ 67,\ 73,\ 79,\ 97 \text{ etc.}$$

COROLLARIUM 3

58. Si ergo numeri cubici per hos numeros primos $3m+1$ dividantur, sequentia residua remanebunt:

Divisores	Residua
7	1, 6
13	1, 5, 8, 12
19	1, 7, 8, 11, 12, 18
31	1, 2, 4, 8, 15, 16, 23, 27, 29, 30
37	1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36
	etc.

In his residuis primo occurrunt omnes cubi divisoribus minores, deinde si quodpiam residuum fuerit r pro divisore $3m+1$, tum quoque aliud dabitur residuum $=3m+1-r$; si enim cubus f^3 dederit residuum r, cubus $(3m+1-f)^3$ dabit residuum $-r$ seu $3m+1-r$.

SCHOLION

59. Notatu hic dignum est numerum residuorum perpetuo esse $=m$, si divisor fuerit $=3m+1$. Semper ergo dantur tres cubi, quorum radices sint $< 3m+1$, ex quibus idem residuum resultat. Scilicet hi tres cubi 1^3, 2^3, 4^3 per 7 divisi idem dant residuum $=1$ et hi tres cubi 2^3, 5^3 et 6^3 per 13 divisi idem dant residuum 8. Praeterea hic notari convenit, si pro a alii valores praeter hos assignatos capiantur, tum a^m-1 non esse per $3m+1$ divisibile; quod etsi verum esse facile deprehenditur, tamen eius demonstratio ex praecedentibus non sequitur pertinetque haec veritas ad id genus, quod nobis nosse, non autem demonstrare licet. His ergo casibus, quibus a^m-1 per $3m+1$ non est divisibile, haec formula $a^{2m}+a^m+1$ divisionem admittet.

THEOREMA 13

60. *Si fuerit* $a=f^n\pm(mn+1)\alpha$ *existente* $mn+1$ *numero primo, tum haec forma* a^m-1 *erit divisibilis per* $mn+1$.

DEMONSTRATIO

Ob $mn+1$ numerum primum erit $f^{mn}-1$ divisibile per $mn+1$. At est $f^{mn}-1=(f^n)^m-1$, unde quoque haec forma $(f^n\pm(mn+1)\alpha)^m-1$ erit divisibilis per $mn+1$. Quare si ponatur $a=f^n\pm(mn+1)\alpha$, haec formula a^m-1 per $mn+1$ dividi poterit. Q. E. D.

COROLLARIUM 1

61. Si ergo potestates exponentis n per numerum primum $mn+1$ dividantur, singula residua vel ipsa vel multiplo ipsius $mn+1$ quocunque aucta idoneos praebebunt valores pro a, ut a^m-1 fiat per $mn+1$ divisibile.

COROLLARIUM 2

62. Hinc si a^m-1 non fuerit per $mn+1$ divisibile, tum valor ipsius a in hac expressione $f^n \pm (mn+1)\alpha$ non continebitur seu nulla dabitur potestas exponentis n, quae per $mn+1$ divisa relinquat a.

SCHOLION

63. Propositionis huius conversa, si omni modo examinetur, quoque vera deprehenditur; ita ut, quoties a^m-1 sit divisibile per $mn+1$, toties quoque valor ipsius a in formula $f^n \pm (mn+1)\alpha$ contineatur; seu toties dabitur potestas f^n, quae per $mn+1$ divisa relinquat a pro residuo. Ita, cum observassem formulam $2^{64}-1$ esse per 641 divisibilem, ob $m=64$ fiet $n=10$, dabitur quoque potestas dignitatis decimae, quae per 641 divisa relinquat 2. Atque revera huiusmodi potestatem deprehendi esse 96^{10}. Praeterea vero cum $2^{32}-1$ non sit divisibile per 641, hoc casu fit $m=32$ et $n=20$; nulla igitur datur potestas dignitatis vicesimae, quae per 641 divisa relinquat 2. Veritas huius posterioris asserti rigorose est evicta, sed adhuc desideratur demonstratio harum propositionum conversarum: scilicet si a^m-1 fuerit divisibile per numerum primum $mn+1$, tum quoque semper a esse numerum in hac formula $f^n \pm (mn+1)\alpha$ comprehensum, atque si a non contineatur in formula $f^n \pm (mn+1)\alpha$, tum quoque a^m-1 per $mn+1$ divisionem non admittere.[1]) Quarum propositionum si altera demonstrari posset, simul veritas alterius esset evicta. Ceterum theorema hic demonstratum huc redit, ut, quoties f^n-a fuerit divisibile per $mn+1$, toties quoque formula a^m-1 sit per $mn+1$ divisibilis. In hoc genere latius patet theorema sequens.

---

1) Demonstrationem harum propositionum conversarum postea EULERUS ipse dedit in Commentatione 262 (§ 72) huius voluminis. F. R.

THEOREMA 14

64. *Si fuerit* $f^n - ag^n$ *divisibile per numerum primum* $mn+1$, *tum quoque* $a^m - 1$ *erit divisibile per* $mn+1$.

DEMONSTRATIO

Cum ponatur formula $f^n - ag^n$ divisibilis per $mn+1$, erit quoque haec formula $f^{mn} - a^m g^{mn}$, quippe quae per illam dividi potest, divisibilis per $mn+1$. At cum $mn+1$ sit numerus primus, per eum divisibilis erit haec forma $f^{mn} - g^{mn}$; unde quoque differentia $g^{mn}(a^m - 1)$ seu ipsa formula $a^m - 1$ per $mn+1$ erit divisibilis, propterea quod g per $mn+1$ divisionem admittere nequeat, nisi simul f per eundem esset divisibile, qui casus in nostro ratiocinio perpetuo excluditur. Q. E. D.

COROLLARIUM 1

65. Si ergo $a^m - 1$ per $mn+1$ non fuerit divisibile, tum quoque nulli dantur numeri f et g, ut haec formula $f^n - ag^n$ per $mn+1$ fiat divisibilis.

COROLLARIUM 2

66. Si superioris propositionis conversa demonstrari posset, tum quoque evictum foret, quoties $f^n - a$ per $mn+1$ dividi nequeat, tum ne hanc quidem formulam $f^n - ag^n$ divisionem per $mn+1$ admittere posse; simul vero etiam pateret, si $f^n - ag^n$ sit divisibile per $mn+1$, tum quoque dari huiusmodi formulam $f^n - a$, quae sit per $mn+1$ divisibilis.

THEOREMA 15

67. *Si huiusmodi formula* $af^n - bg^n$ *fuerit divisibilis per numerum primum* $mn+1$, *tum quoque haec formula* $a^m - b^m$ *erit per* $mn+1$ *divisibilis.*

DEMONSTRATIO

Si fuerit $af^n - bg^n$ divisibile per $mn+1$, tum quoque haec formula $a^m f^{mn} - b^m g^{mn}$ erit per $mn+1$ divisibilis. At ob $mn+1$ numerum primum

erit quoque haec formula $f^{mn} - g^{mn}$ ideoque et haec $a^m f^{mn} - a^m g^{mn}$ per $mn+1$ divisibilis; subtrahatur haec ab illa $a^m f^{mn} - b^m g^{mn}$ atque residuum $g^{mn}(a^m - b^m)$ seu $a^m - b^m$ per $mn+1$ erit divisibile. Q. E. D.

COROLLARIUM 1

68. Si itaque $a^m - b^m$ non fuerit per $mn+1$ divisibile, tum nulli dabuntur numeri pro f et g substituendi, ut huiusmodi formula $af^n - bg^n$ sit per $mn+1$ divisibilis.

COROLLARIUM 2

69. Huius propositionis conversa, quod, si fuerit formula $a^m - b^m$ divisibilis per $mn+1$, simul dentur numeri f et g, ut $af^n - bg^n$ fiat divisibilis per $mn+1$, utcunque examinetur, vera deprehenditur. Interim tamen eius demonstratio etiamnum desideratur.

SCHOLION

70. Casus huius propositionis inversae demonstrari potest, quo numeri m et n sunt inter se primi; hoc enim casu semper eiusmodi numeri μ et ν exhiberi possunt, ut sit $\mu n \pm 1 = \nu m$. Namque si inter numeros m et n ea operatio instituatur, quae pro maximo communi divisore institui solet, atque quoti notentur ex iisque fractiones ad $\frac{m}{n}$ appropinquantes quaerantur, ultima erit $\frac{m}{n}$, et si penultima fuerit $\frac{\mu}{\nu}$, erit $\mu n \pm 1 = \nu m$. Hoc ergo lemmate praemisso demonstratio propositionis conversae, qua m et n sunt numeri inter se primi, ita se habebit.

THEOREMA 16

71. *Si m et n fuerint numeri primi inter se atque ista formula $a^m - b^m$ divisibilis sit per numerum $mn+1$, tum dabitur formula $af^n - bg^n$ divisibilis per $mn+1$.*

DEMONSTRATIO

Ponatur $f = a^\mu$ et $g = b^\mu$ atque formula $af^n - bg^n$ abibit in hanc $a^{\mu n+1} - b^{\mu n+1}$; quare si μ ita capiatur, ut sit $\mu n + 1 = \nu m$, habebitur $a^{\nu m} - b^{\nu m}$;

quae cum sit divisibilis per $a^m - b^m$, quoque per $mn + 1$ divisibilis erit sicque dabitur casus, quo $af^n - bg^n$ divisibile erit per $mn + 1$.

Sin autem fuerit $\mu n - 1 = \nu m$, tum sumatur $f = b^\mu$ et $g = a^\mu$ fietque $af^n - bg^n = ab^{\mu n} - ba^{\mu n} = ab(b^{\mu n - 1} - a^{\mu n - 1}) = - ab(a^{\nu m} - b^{\nu m})$ ideoque erit per $mn + 1$ divisibilis. Q. E. D.

COROLLARIUM 1

72. Si ergo m et n fuerint numeri inter se primi atque $mn+1$ numerus primus, tum istae propositiones sunt demonstratae:

I. *Si* $af^n - bg^n$ *fuerit divisibile per* $mn + 1$, *tum quoque* $a^m - b^m$ *erit per* $mn + 1$ *divisibile, et si illa formula nullo modo sit divisibilis per* $mn + 1$, *tum etiam haec non erit divisibilis.*

II. *Si* $a^m - b^m$ *fuerit divisibile per* $mn + 1$, *tum dabitur numerus huius formae* $af^n - bg^n$ *per* $mn + 1$ *divisibilis, atque si* $a^m - b^m$ *per* $mn + 1$ *divisionem non admittat, tum nullus dabitur numerus formae* $af^n - bg^n$ *per* $mn + 1$ *divisibilis.*

COROLLARIUM 2

73. Si m sit numerus par, tum b aeque negative atque affirmative accipi potest; hoc ergo casu si $a^m - b^m$ fuerit divisibile per $mn+1$, tum etiam eiusmodi formula $af^n + bg^n$ per $mn+1$ divisibilis assignari poterit; id quod etiam inde patet, quod n sit numerus impar ideoque potestas g^n negativa fieri queat.

COROLLARIUM 3

74. Simili modo demonstrabitur, si fuerint ut ante m et n numeri inter se primi atque haec formula $a^m - b^m$ sit divisibilis per $mp + 1$, tum quoque exhiberi posse formulam huiusmodi $af^n - bg^n$ divisibilem per $mp + 1$.

DE NUMERIS AMICABILIBUS[1])

Commentatio 152 indicis ENESTROEMIANI
Opuscula varii argumenti 2, 1750, p. 23—107

DEFINITIO

1. *Bini numeri vocantur amicabiles, si ita sint comparati, ut summa partium aliquotarum unius aequalis sit alteri numero et vicissim summa partium aliquotarum alterius priori numero aequetur.*

Sic isti numeri 220 et 284 sunt amicabiles; prioris enim 220 partes aliquotae iunctim sumtae

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110$$

faciunt 284 et huius numeri 284 partes aliquotae

$$1 + 2 + 4 + 71 + 142$$

producunt priorem numerum 220.

SCHOLION

2. STIFELIUS[2]), qui primus[3]) huiusmodi numerorum mentionem fecit, casu hos duos numeros 220 et 284 contemplatus ad hanc speculationem deductus videtur; Analysin enim ineptam existimat, cuius ope plura istiusmodi numerorum paria inveniantur. CARTESIUS[3]) vero Analysin ad hoc negotium accommodare est conatus regulamque tradidit, qua tria talium numerorum paria

1) Cf. Commentationes 100 et 798 in hoc vol. 2 et in vol. 5 contentas. Vide etiam G. W. KRAFFT, *De numeris amicabilibus atque aliis ad hanc doctrinam spectantibus*, Novi comment. acad. sc. Petrop. 2 (1749), 1751, p. 100, nec non epistolas, quas a. 1746 KRAFFT ad EULERUM scripsit, *LEONHARDI EULERI Opera omnia*, series III. F. R.

2) M. STIFEL, *Arithmetica integra*, Norimbergae, 1544, fol. 10^{v}. F. R.

3) Sed vide notam 1 p. 60. F. R.

elicuit, neque praeter ea SCHOTENIUS[1]), qui multum in hac investigatione desudasse videtur, plura eruere valuit. Post haec tempora nemo fere Geometrarum ad hanc quaestionem magis evolvendam operam impendisse reperitur. Cum autem nullum sit dubium, quin Analysis quoque ex hac parte incrementa non contemnenda sit consecutura, si methodus aperiatur, qua multo plura huiusmodi numerorum paria investigare liceat, haud abs re fore arbitror, si methodos quasdam huc spectantes, in quas forte incidi, communicavero. In hunc finem autem sequentia praemittere necesse est.

HYPOTHESIS

3. *Si n denotet numerum quemcunque integrum positivum, cuiusmodi numeri hic semper sunt intelligendi, omnium eius divisorum summam hoc signo $\int n$ indicabo, ita ut character $\int$ numero cuipiam praefixus summam omnium eiusdem numeri divisorum denotet; sic erit $\int 6 = 1 + 2 + 3 + 6 = 12$.*

COROLLARIUM 1

4. Quoniam inter divisores cuiusvis numeri hic ipse numerus refertur, partes aliquotae autem censentur divisores ipso numero excepto, manifestum est summam partium aliquotarum numeri n exprimi per $\int n - n$.

COROLLARIUM 2

5. Quoniam numerus primus nullos alios divisores admittit praeter unitatem et se ipsum, si n sit numerus primus, erit $\int n = 1 + n$. Cum autem casu $n = 1$ sit $\int 1 = 1$, patet unitatem non recte numeris primis annumerari.

LEMMA 1

6. *Si m et n fuerint numeri inter se primi, ut praeter unitatem nullum habeant divisorem communem, tum erit $\int mn = \int m \cdot \int n$ seu summa divisorum producti mn aequalis est producto ex summis divisorum utriusque numeri m et n.*

1) Vide notam 1 p. 60. F. R

Productum enim mn primo habet singulos divisores utriusque factoris m et n, tum vero insuper divisibile est per producta ex singulis divisoribus numeri m in singulos divisores numeri n. Hi vero omnes ipsius mn divisores iunctim prodeunt, si $\int m$ per $\int n$ multiplicetur.

COROLLARIUM 1

7. Si numerorum m et n uterque sit primus ideoque $\int m = 1 + m$ et $\int n = 1 + n$, erit summa divisorum producti

$$\int mn = (1+m)(1+n) = 1 + m + n + mn.$$

Si praeterea p sit numerus primus diversus ab m et n, erit

$$\int mnp = \int mn \cdot \int p = \int m \cdot \int n \cdot \int p = (1+m)(1+n)(1+p).$$

Hincque summa divisorum cuiusque numeri, qui est productum ex quotcunque numeris primis diversis, facile assignabitur.

COROLLARIUM 2

8. Si m, n et p non quidem sint numeri primi, sed tamen eiusmodi, ut praeter unitatem nullum habeant divisorem communem, tum mn et p erunt numeri inter se primi ac propterea $\int mnp = \int mn \cdot \int p$. Cum autem sit $\int mn = \int m \cdot \int n$, erit $\int mnp = \int m \cdot \int n \cdot \int p$.

SCHOLION

9. Nisi factores m, n, p sint numeri inter se primi, summa divisorum producti, prout per lemma indicatur, non est iusta. Cum enim secundum lemma singuli divisores factorum m, n, p inter divisores producti mnp referantur, si haberent divisorem communem, is inter divisores producti bis numeraretur; at dum quaestio de summa divisorum cuiuspiam numeri instituitur, nullum divisorem bis numerare oportet. Hinc si m et n sint numeri primi ac $m = n$, non erit $\int nn = \int n \cdot \int n = (1+n)^2 = 1 + 2n + nn$, sed habebitur $\int nn = 1 + n + nn$ neque divisorem n bis poni convenit. Cum igitur per hoc lemma summa divisorum cuiusque numeri, qui est productum ex quotcunque numeris primis diversis, recte assignetur, residuum est, ut pro factoribus aequalibus regula tradatur, cuius ope summa divisorum producti definiri queat.

LEMMA 2

10. *Si n sit numerus primus, erit* $\int n^2 = 1 + n + n^2$, $\int n^3 = 1 + n + n^2 + n^3$, $n^4 = 1 + n + n^2 + n^3 + n^4$ *et generatim erit* $\int n^k = 1 + n + n^2 + \cdots + n^k = \frac{n^{k+1} - 1}{n - 1}$.

COROLLARIUM 1

11. Cum sit $\int n = 1 + n$, erit $\int n^2 = \int n + n^2$ vel etiam $\int n^2 = 1 + n \int n$. Simili modo erit $\int n^3 = \int n^2 + n^3$ vel etiam $\int n^3 = 1 + n \int n^2$; porroque $\int n^4 = \int n^3 + n^4$ seu $\int n^4 = 1 + n \int n^3$, et ita porro. Sicque ex cognita summa divisorum cuiusque potestatis n^k facile summa divisorum potestatis sequentis n^{k+1} assignatur, cum sit $\int n^{k+1} = \int n^k + n^{k+1}$ seu $\int n^{k+1} = 1 + n \int n^k$.

COROLLARIUM 2

12. Quo summae divisorum facilius per factores exprimi queant, notandum est esse

$$\int n^3 = (1 + n)(1 + n^2) = (1 + n^2) \int n,$$

$$\int n^5 = (1 + n^2 + n^4) \int n, \qquad \int n^7 = (1 + n^2 + n^4 + n^6) \int n = (1 + n^4)(1 + n^2) \int n;$$

sicque summae divisorum potestatum imparium semper per factores exhiberi possunt, at potestatum parium summae divisorum quandoque erunt numeri primi.

COROLLARIUM 3

13. Hinc igitur facile tabula condi poterit, qua non solum numerorum primorum, sed etiam potestatum ipsorum summae divisorum exhibeantur. Cuiusmodi tabulam hic adiicere visum est, in qua omnium numerorum primorum millenario non maiorum eorumque potestatum ad tertiam usque et altiores pro minoribus numeris summae divisorum per factores expressae traduntur.[1])

1) In editione principe tabula sequens nonnullos errores continet, qui omnes etiam in *Commentationibus arithmeticis* (ed. P. H. et N. Fuss) inveniuntur, hac in editione autem correcti sunt. Quae correctiones pertinent ad numeros 5^5, 37^3, 41^3, 149^3, 173^2, 283^3, 461^3, 523^3, 563^3, 571^3, 613^2, 769^3, 811, 827. Praeterea addendae erant summae divisorum numerorum 79, 79^2, 79^3, quae in duabus prioribus editionibus omissae sunt (sed vide Prooemium *Comment. arithm.*, p. LXXXI). F. R.

Num.	Summa divisorum
2	3
2^2	7
2^3	$3 \cdot 5$
2^4	31
2^5	$3^2 \cdot 7$
2^6	127
2^7	$3 \cdot 5 \cdot 17$
2^8	$7 \cdot 73$
2^9	$3 \cdot 11 \cdot 31$
2^{10}	$23 \cdot 89$
2^{11}	$3^2 \cdot 5 \cdot 7 \cdot 13$
2^{12}	8191
2^{13}	$3 \cdot 43 \cdot 127$
2^{14}	$7 \cdot 31 \cdot 151$
2^{15}	$3 \cdot 5 \cdot 17 \cdot 257$
2^{16}	131071
2^{17}	$3^3 \cdot 7 \cdot 19 \cdot 73$
2^{18}	524287
2^{19}	$3 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41$
2^{20}	$7^2 \cdot 127 \cdot 337$
2^{21}	$3 \cdot 23 \cdot 89 \cdot 683$
2^{22}	$47 \cdot 178481$
2^{23}	$3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$
2^{24}	$31 \cdot 601 \cdot 1801$
2^{25}	$3 \cdot 2731 \cdot 8191$
2^{26}	$7 \cdot 73 \cdot 262657$
2^{27}	$3 \cdot 5 \cdot 29 \cdot 43 \cdot 113 \cdot 127$
2^{28}	$233 \cdot 1103 \cdot 2089$
2^{29}	$3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331$
2^{30}	2147483647
2^{31}	$3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537$
2^{32}	$7 \cdot 23 \cdot 89 \cdot 599479$
2^{33}	$3 \cdot 43691 \cdot 131071$
2^{34}	$31 \cdot 71 \cdot 127 \cdot 122921$
2^{35}	$3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 73 \cdot 109$
2^{36}	$223 \cdot 616318177$

Num.	Summa divisorum
3	2^2
3^2	13
3^3	$2^3 \cdot 5$
3^4	11^2
3^5	$2^2 \cdot 7 \cdot 13$
3^6	1093
3^7	$2^4 \cdot 5 \cdot 41$
3^8	$13 \cdot 757$
3^9	$2^2 \cdot 11^2 \cdot 61$
3^{10}	$23 \cdot 3851$
3^{11}	$2^3 \cdot 5 \cdot 7 \cdot 13 \cdot 73$
3^{12}	797161
3^{13}	$2^2 \cdot 547 \cdot 1093$
3^{14}	$11^2 \cdot 13 \cdot 4561$
3^{15}	$2^5 \cdot 5 \cdot 17 \cdot 41 \cdot 193$
5	$2 \cdot 3$
5^2	31
5^3	$2^2 \cdot 3 \cdot 13$
5^4	$11 \cdot 71$
5^5	$2 \cdot 3^2 \cdot 7 \cdot 31$
5^6	19531
5^7	$2^3 \cdot 3 \cdot 13 \cdot 313$
5^8	$19 \cdot 31 \cdot 829$
5^9	$2 \cdot 3 \cdot 11 \cdot 71 \cdot 521$
7	2^3
7^2	$3 \cdot 19$
7^3	$2^4 \cdot 5^2$
7^4	2801
7^5	$2^3 \cdot 3 \cdot 19 \cdot 43$
7^6	$29 \cdot 4733$
7^7	$2^5 \cdot 5^2 \cdot 1201$
7^8	$3^2 \cdot 19 \cdot 37 \cdot 1063$
7^9	$2^3 \cdot 11 \cdot 191 \cdot 2801$
7^{10}	329554457

Num.	Summa divisorum
11	$2^2 \cdot 3$
11^2	$7 \cdot 19$
11^3	$2^3 \cdot 3 \cdot 61$
11^4	$5 \cdot 3221$
11^5	$2^2 \cdot 3^2 \cdot 7 \cdot 19 \cdot 37$
11^6	$43 \cdot 45319$
11^7	$2^4 \cdot 3 \cdot 61 \cdot 7321$
11^8	$7 \cdot 19 \cdot 1772893$
11^9	$2^2 \cdot 3 \cdot 5 \cdot 3221 \cdot 13421$
13	$2 \cdot 7$
13^2	$3 \cdot 61$
13^3	$2^2 \cdot 5 \cdot 7 \cdot 17$
13^4	30941
13^5	$2 \cdot 3 \cdot 7 \cdot 61 \cdot 157$
13^6	5229043
13^7	$2^3 \cdot 5 \cdot 7 \cdot 17 \cdot 14281$
17	$2 \cdot 3^2$
17^2	307
17^3	$2^2 \cdot 3^2 \cdot 5 \cdot 29$
17^4	88741
17^5	$2 \cdot 3^3 \cdot 7 \cdot 13 \cdot 307$
19	$2^2 \cdot 5$
19^2	$3 \cdot 127$
19^3	$2^3 \cdot 5 \cdot 181$
19^4	$151 \cdot 911$
19^5	$2^2 \cdot 3 \cdot 5 \cdot 7^3 \cdot 127$
23	$2^3 \cdot 3$
23^2	$7 \cdot 79$
23^3	$2^4 \cdot 3 \cdot 5 \cdot 53$
23^4	292561
29	$2 \cdot 3 \cdot 5$
29^2	$13 \cdot 67$
29^3	$2^2 \cdot 3 \cdot 5 \cdot 421$

Num.	Summa divisorum	Num.	Summa divisorum	Num.	Summa divisorum
31	2^5	79	$2^4 \cdot 5$	137	$2 \cdot 3 \cdot 23$
31^2	$3 \cdot 331$	79^2	$3 \cdot 7^2 \cdot 43$	137^2	$7 \cdot 37 \cdot 73$
31^3	$2^6 \cdot 13 \cdot 37$	79^3	$2^5 \cdot 5 \cdot 3121$	137^3	$2^2 \cdot 3 \cdot 5 \cdot 23 \cdot 1877$
37	$2 \cdot 19$	83	$2^2 \cdot 3 \cdot 7$	139	$2^2 \cdot 5 \cdot 7$
37^2	$3 \cdot 7 \cdot 67$	83^2	$19 \cdot 367$	139^2	$3 \cdot 13 \cdot 499$
37^3	$2^2 \cdot 5 \cdot 19 \cdot 137$	83^3	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 53$	139^3	$2^3 \cdot 5 \cdot 7 \cdot 9661$
41	$2 \cdot 3 \cdot 7$	89	$2 \cdot 3^2 \cdot 5$	149	$2 \cdot 3 \cdot 5^2$
41^2	1723	89^2	8011	149^2	$7 \cdot 31 \cdot 103$
41^3	$2^2 \cdot 3 \cdot 7 \cdot 29^2$	89^3	$2^2 \cdot 3^2 \cdot 5 \cdot 17 \cdot 233$	149^3	$2^2 \cdot 3 \cdot 5^2 \cdot 17 \cdot 653$
43	$2^2 \cdot 11$	97	$2 \cdot 7^2$	151	$2^3 \cdot 19$
43^2	$3 \cdot 631$	97^2	$3 \cdot 3169$	151^2	$3 \cdot 7 \cdot 1093$
43^3	$2^3 \cdot 5^2 \cdot 11 \cdot 37$	97^3	$2^2 \cdot 5 \cdot 7^2 \cdot 941$	151^3	$2^4 \cdot 13 \cdot 19 \cdot 877$
47	$2^4 \cdot 3$	101	$2 \cdot 3 \cdot 17$	157	$2 \cdot 79$
47^2	$37 \cdot 61$	101^2	10303	157^2	$3 \cdot 8269$
47^3	$2^5 \cdot 3 \cdot 5 \cdot 13 \cdot 17$	101^3	$2^2 \cdot 3 \cdot 17 \cdot 5101$	157^3	$2^2 \cdot 5^2 \cdot 17 \cdot 29 \cdot 79$
53	$2 \cdot 3^3$	103	$2^3 \cdot 13$	163	$2^2 \cdot 41$
53^2	$7 \cdot 409$	103^2	$3 \cdot 3571$	163^2	$3 \cdot 7 \cdot 19 \cdot 67$
53^3	$2^2 \cdot 3^3 \cdot 5 \cdot 281$	103^3	$2^4 \cdot 5 \cdot 13 \cdot 1061$	163^3	$2^3 \cdot 5 \cdot 41 \cdot 2657$
59	$2^2 \cdot 3 \cdot 5$	107	$2^2 \cdot 3^3$	167	$2^3 \cdot 3 \cdot 7$
59^2	3541	107^2	$7 \cdot 13 \cdot 127$	167^2	28057
59^3	$2^3 \cdot 3 \cdot 5 \cdot 1741$	107^3	$2^3 \cdot 3^3 \cdot 5^2 \cdot 229$	167^3	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 2789$
61	$2 \cdot 31$	109	$2 \cdot 5 \cdot 11$	173	$2 \cdot 3 \cdot 29$
61^2	$3 \cdot 13 \cdot 97$	109^2	$3 \cdot 7 \cdot 571$	173^2	30103
61^3	$2^2 \cdot 31 \cdot 1861$	109^3	$2^2 \cdot 5 \cdot 11 \cdot 13 \cdot 457$	173^3	$2^2 \cdot 3 \cdot 5 \cdot 29 \cdot 41 \cdot 73$
67	$2^2 \cdot 17$	113	$2 \cdot 3 \cdot 19$	179	$2^2 \cdot 3^2 \cdot 5$
67^2	$3 \cdot 7^2 \cdot 31$	113^2	$13 \cdot 991$	179^2	$7 \cdot 4603$
67^3	$2^3 \cdot 5 \cdot 17 \cdot 449$	113^3	$2^2 \cdot 3 \cdot 5 \cdot 19 \cdot 1277$	179^3	$2^3 \cdot 3^2 \cdot 5 \cdot 37 \cdot 433$
71	$2^3 \cdot 3^2$	127	2^7	181	$2 \cdot 7 \cdot 13$
71^2	5113	127^2	$3 \cdot 5419$	181^2	$3 \cdot 79 \cdot 139$
71^3	$2^4 \cdot 3^2 \cdot 2521$	127^3	$2^8 \cdot 5 \cdot 1613$	181^3	$2^2 \cdot 7 \cdot 13 \cdot 16381$
73	$2 \cdot 37$	131	$2^2 \cdot 3 \cdot 11$	191	$2^6 \cdot 3$
73^2	$3 \cdot 1801$	131^2	17293	191^2	$7 \cdot 13^2 \cdot 31$
73^3	$2^2 \cdot 5 \cdot 13 \cdot 37 \cdot 41$	131^3	$2^3 \cdot 3 \cdot 11 \cdot 8581$	191^3	$2^7 \cdot 3 \cdot 17 \cdot 29 \cdot 37$

Num.	Summa divisorum	Num.	Summa divisorum	Num.	Summa divisorum
193	$2\cdot97$	257	$2\cdot3\cdot43$	317	$2\cdot3\cdot53$
193^2	$3\cdot7\cdot1783$	257^2	$61\cdot1087$	317^2	$7\cdot14401$
193^3	$2^2\cdot5^3\cdot97\cdot149$	257^3	$2^2\cdot3\cdot5^2\cdot43\cdot1321$	317^3	$2^2\cdot3\cdot5\cdot13\cdot53\cdot773$
197	$2\cdot3^2\cdot11$	263	$2^3\cdot3\cdot11$	331	$2^2\cdot83$
197^2	$19\cdot2053$	263^2	$7^2\cdot13\cdot109$	331^2	$3\cdot7\cdot5233$
197^3	$2^2\cdot3^2\cdot5\cdot11\cdot3881$	263^3	$2^4\cdot3\cdot5\cdot11\cdot6917$	331^3	$2^3\cdot29\cdot83\cdot1889$
199	$2^3\cdot5^2$	269	$2\cdot3^3\cdot5$	337	$2\cdot13^2$
199^2	$3\cdot13267$	269^2	$13\cdot37\cdot151$	337^2	$3\cdot43\cdot883$
199^3	$2^4\cdot5^2\cdot19801$	269^3	$2^2\cdot3^3\cdot5\cdot97\cdot373$	337^3	$2^2\cdot5\cdot13^2\cdot41\cdot277$
211	$2^2\cdot53$	271	$2^4\cdot17$	347	$2^2\cdot3\cdot29$
211^2	$3\cdot13\cdot31\cdot37$	271^2	$3\cdot24571$	347^2	$7\cdot13\cdot1327$
211^3	$2^3\cdot53\cdot113\cdot197$	271^3	$2^5\cdot17\cdot36721$	347^3	$2^3\cdot3\cdot5\cdot29\cdot12041$
223	$2^5\cdot7$	277	$2\cdot139$	349	$2\cdot5^2\cdot7$
223^2	$3\cdot16651$	277^2	$3\cdot7\cdot19\cdot193$	349^2	$3\cdot19\cdot2143$
223^3	$2^6\cdot5\cdot7\cdot4973$	277^3	$2^2\cdot5\cdot139\cdot7673$	349^3	$2^2\cdot5^2\cdot7\cdot60901$
227	$2^2\cdot3\cdot19$	281	$2\cdot3\cdot47$	353	$2\cdot3\cdot59$
227^2	$73\cdot709$	281^2	$109\cdot727$	353^2	$19\cdot6577$
227^3	$2^3\cdot3\cdot5\cdot19\cdot5153$	281^3	$2^2\cdot3\cdot13\cdot47\cdot3037$	353^3	$2^2\cdot3\cdot5\cdot17\cdot59\cdot733$
229	$2\cdot5\cdot23$	283	$2^2\cdot71$	359	$2^3\cdot3^2\cdot5$
229^2	$3\cdot97\cdot181$	283^2	$3\cdot73\cdot367$	359^2	$7\cdot37\cdot499$
229^3	$2^2\cdot5\cdot13\cdot23\cdot2017$	283^3	$2^3\cdot5\cdot71\cdot8009$	359^3	$2^4\cdot3^2\cdot5\cdot13\cdot4957$
233	$2\cdot3^2\cdot13$	293	$2\cdot3\cdot7^2$	367	$2^4\cdot23$
233^2	$7\cdot7789$	293^2	86143	367^2	$3\cdot13\cdot3463$
233^3	$2^2\cdot3^2\cdot5\cdot13\cdot61\cdot89$	293^3	$2^2\cdot3\cdot5^2\cdot7^2\cdot17\cdot101$	367^3	$2^5\cdot5\cdot23\cdot13469$
239	$2^4\cdot3\cdot5$	307	$2^2\cdot7\cdot11$	373	$2\cdot11\cdot17$
239^2	19.3019	307^2	$3\cdot43\cdot733$	373^2	$3\cdot7^2\cdot13\cdot73$
239^3	$2^5\cdot3\cdot5\cdot13^4$	307^3	$2^3\cdot5^3\cdot7\cdot11\cdot13\cdot29$	373^3	$2^2\cdot5\cdot11\cdot17\cdot13913$
241	$2\cdot11^2$	311	$2^3\cdot3\cdot13$	379	$2^2\cdot5\cdot19$
241^2	$3\cdot19441$	311^2	$19\cdot5107$	379^2	$3\cdot61\cdot787$
241^3	$2^2\cdot11^2\cdot113\cdot257$	311^3	$2^4\cdot3\cdot13\cdot137\cdot353$	379^3	$2^3\cdot5\cdot19\cdot71821$
251	$2^2\cdot3^2\cdot7$	313	$2\cdot157$	383	$2^7\cdot3$
251^2	$43\cdot1471$	313^2	$3\cdot181^2$	383^2	147073
251^3	$2^3\cdot3^2\cdot7\cdot17^2\cdot109$	313^3	$2^2\cdot5\cdot97\cdot101\cdot157$	383^3	$2^8\cdot3\cdot5\cdot14669$

Num.	Summa divisorum	Num.	Summa divisorum	Num.	Summa divisorum
389	$2\cdot3\cdot5\cdot13$	457	$2\cdot229$	523	$2^2\cdot131$
389^2	$7\cdot21673$	457^2	$3\cdot7\cdot9967$	523^2	$3\cdot13\cdot7027$
389^3	$2^2\cdot3\cdot5\cdot13\cdot29\cdot2609$	457^3	$2^2\cdot5^2\cdot229\cdot4177$	523^3	$2^3\cdot5\cdot17\cdot131\cdot1609$
397	$2\cdot199$	461	$2\cdot3\cdot7\cdot11$	541	$2\cdot271$
397^2	$3\cdot31\cdot1699$	461^2	$373\cdot571$	541^2	$3\cdot7\cdot13963$
397^3	$2^2\cdot5\cdot199\cdot15761$	461^3	$2^2\cdot3\cdot7\cdot11\cdot106261$	541^3	$2^2\cdot13\cdot271\cdot11257$
401	$2\cdot3\cdot67$	463	$2^4\cdot29$	547	$2^2\cdot137$
401^2	$7\cdot23029$	463^2	$3\cdot19\cdot3769$	547^2	$3\cdot163\cdot613$
401^3	$2^2\cdot3\cdot37\cdot41\cdot53\cdot67$	463^3	$2^5\cdot5\cdot13\cdot17\cdot29\cdot97$	547^3	$2^3\cdot5\cdot137\cdot29921$
409	$2\cdot5\cdot41$	467	$2^2\cdot3^2\cdot13$	557	$2\cdot3^2\cdot31$
409^2	$3\cdot55897$	467^2	$19\cdot11503$	557^2	$7^2\cdot6343$
409^3	$2^2\cdot5\cdot41\cdot83641$	467^3	$2^3\cdot3^2\cdot5\cdot13\cdot113\cdot193$	557^3	$2^2\cdot3^2\cdot5^3\cdot17\cdot31\cdot73$
419	$2^2\cdot3\cdot5\cdot7$	479	$2^5\cdot3\cdot5$	563	$2^2\cdot3\cdot47$
419^2	$13\cdot13537$	479^2	$43\cdot5347$	563^2	$31\cdot10243$
419^3	$2^3\cdot3\cdot5\cdot7\cdot41\cdot2141$	479^3	$2^6\cdot3\cdot5\cdot89\cdot1289$	563^3	$2^3\cdot3\cdot5\cdot29\cdot47\cdot1093$
421	$2\cdot211$	487	$2^3\cdot61$	569	$2\cdot3\cdot5\cdot19$
421^2	$3\cdot59221$	487^2	$3\cdot7\cdot11317$	569^2	$7^2\cdot6619$
421^3	$2^2\cdot13\cdot17\cdot211\cdot401$	487^3	$2^4\cdot5\cdot37\cdot61\cdot641$	569^3	$2^2\cdot3\cdot5\cdot19\cdot161881$
431	$2^4\cdot3^3$	491	$2^2\cdot3\cdot41$	571	$2^2\cdot11\cdot13$
431^2	$7\cdot67\cdot397$	491^2	$37\cdot6529$	571^2	$3\cdot7\cdot103\cdot151$
431^3	$2^5\cdot3^3\cdot293\cdot317$	491^3	$2^3\cdot3\cdot41\cdot149\cdot809$	571^3	$2^3\cdot11\cdot13\cdot163021$
433	$2\cdot7\cdot31$	499	$2^2\cdot5^3$	577	$2\cdot17^2$
433^2	$3\cdot37\cdot1693$	499^2	$3\cdot7\cdot109^2$	577^2	$3\cdot19\cdot5851$
433^3	$2^2\cdot5\cdot7\cdot31\cdot18749$	499^3	$2^3\cdot5^3\cdot13\cdot61\cdot157$	577^3	$2^2\cdot5\cdot13^2\cdot17^2\cdot197$
439	$2^3\cdot5\cdot11$	503	$2^3\cdot3^2\cdot7$	587	$2^2\cdot3\cdot7^2$
439^2	$3\cdot31^2\cdot67$	503^2	$13\cdot19501$	587^2	$547\cdot631$
439^3	$2^4\cdot5\cdot11\cdot173\cdot557$	503^3	$2^4\cdot3^2\cdot5\cdot7\cdot25301$	587^3	$2^3\cdot3\cdot5\cdot7^2\cdot34457$
443	$2^2\cdot3\cdot37$	509	$2\cdot3\cdot5\cdot17$	593	$2\cdot3^3\cdot11$
443^2	$7\cdot28099$	509^2	$43\cdot6037$	593^2	$163\cdot2161$
443^3	$2^3\cdot3\cdot5^4\cdot37\cdot157$	509^3	$2^2\cdot3\cdot5\cdot17\cdot281\cdot461$	593^3	$2^2\cdot3^3\cdot5^2\cdot11\cdot13\cdot541$
449	$2\cdot3^2\cdot5^2$	521	$2\cdot3^2\cdot29$	599	$2^3\cdot3\cdot5^2$
449^2	$97\cdot2083$	521^2	$31^2\cdot283$	599^2	$7\cdot51343$
449^3	$2^2\cdot3^2\cdot5^2\cdot100801$	521^3	$2^2\cdot3^2\cdot29\cdot135721$	599^3	$2^4\cdot3\cdot5^2\cdot17\cdot61\cdot173$

Num.	Summa divisorum	Num.	Summa divisorum	Num.	Summa divisorum
601	$2\cdot7\cdot43$	661	$2\cdot331$	743	$2^3\cdot3\cdot31$
601^2	$3\cdot13\cdot9277$	661^2	$3\cdot145861$	743^2	552793
601^3	$2^2\cdot7\cdot43\cdot313\cdot577$	661^3	$2^2\cdot331\cdot218461$	743^3	$2^4\cdot3\cdot5^2\cdot31\cdot61\cdot181$
607	$2^5\cdot19$	673	$2\cdot337$	751	$2^4\cdot47$
607^2	$3\cdot13\cdot9463$	673^2	$3\cdot151201$	751^2	$3\cdot7\cdot26893$
607^3	$2^6\cdot5^2\cdot19\cdot7369$	673^3	$2^2\cdot5\cdot337\cdot45293$	751^3	$2^5\cdot47\cdot282001$
613	$2\cdot307$	677	$2\cdot3\cdot113$	757	$2\cdot379$
613^2	$3\cdot7\cdot17923$	677^2	459007	757^2	$3\cdot13\cdot14713$
613^3	$2^2\cdot5\cdot53\cdot307\cdot709$	677^3	$2^2\cdot3\cdot5\cdot113\cdot45833$	757^3	$2^2\cdot5^2\cdot73\cdot157\cdot379$
617	$2\cdot3\cdot103$	683	$2^2\cdot3^2\cdot19$	761	$2\cdot3\cdot127$
617^2	$97\cdot3931$	683^2	$7\cdot66739$	761^2	579883
617^3	$2^2\cdot3\cdot5\cdot103\cdot38069$	683^3	$2^3\cdot3^2\cdot5\cdot19\cdot46649$	761^3	$2^2\cdot3\cdot17\cdot127\cdot17033$
619	$2^2\cdot5\cdot31$	691	$2^2\cdot173$	769	$2\cdot5\cdot7\cdot11$
619^2	$3\cdot19\cdot6733$	691^2	$3\cdot19\cdot8389$	769^2	$3\cdot31\cdot6367$
619^3	$2^3\cdot5\cdot13\cdot31\cdot14737$	691^3	$2^3\cdot173\cdot193\cdot1237$	769^3	$2^2\cdot5\cdot7\cdot11\cdot17\cdot17393$
631	$2^3\cdot79$	701	$2\cdot3^3\cdot13$	773	$2\cdot3^2\cdot43$
631^2	$3\cdot307\cdot433$	701^2	492103	773^2	598303
631^3	$2^4\cdot79\cdot199081$	701^3	$2^2\cdot3^3\cdot13\cdot17\cdot97\cdot149$	773^3	$2^2\cdot3^2\cdot5\cdot43\cdot59753$
641	$2\cdot3\cdot107$	709	$2\cdot5\cdot71$	787	$2^2\cdot197$
641^2	$7\cdot58789$	709^2	$3\cdot7\cdot23971$	787^2	$3\cdot37^2\cdot151$
641^3	$2^2\cdot3\cdot107\cdot205441$	709^3	$2^2\cdot5\cdot37\cdot71\cdot6793$	787^3	$2^3\cdot5\cdot197\cdot241\cdot257$
643	$2^2\cdot7\cdot23$	719	$2^4\cdot3^2\cdot5$	797	$2\cdot3\cdot7\cdot19$
643^2	$3\cdot97\cdot1423$	719^2	$487\cdot1063$	797^2	$157\cdot4051$
643^3	$2^3\cdot5^2\cdot7\cdot23\cdot8269$	719^3	$2^5\cdot3^2\cdot5\cdot53\cdot4877$	797^3	$2^2\cdot3\cdot5\cdot7\cdot19\cdot63521$
647	$2^3\cdot3^4$	727	$2^3\cdot7\cdot13$	809	$2\cdot3^4\cdot5$
647^2	$211\cdot1987$	727^2	$3\cdot176419$	809^2	$7\cdot13\cdot19\cdot379$
647^3	$2^4\cdot3^4\cdot5\cdot41\cdot1021$	727^3	$2^4\cdot5\cdot7\cdot13\cdot17\cdot3109$	809^3	$2^2\cdot3^4\cdot5\cdot229\cdot1429$
653	$2\cdot3\cdot109$	733	$2\cdot367$	811	$2^2\cdot7\cdot29$
653^2	$7\cdot13^2\cdot19^2$	733^2	$3\cdot19\cdot9439$	811^2	$3\cdot31\cdot73\cdot97$
653^3	$2^2\cdot3\cdot5\cdot109\cdot42641$	733^3	$2^2\cdot5\cdot13\cdot367\cdot4133$	811^3	$2^3\cdot7\cdot13\cdot29\cdot41\cdot617$
659	$2^2\cdot3\cdot5\cdot11$	739	$2^2\cdot5\cdot37$	821	$2\cdot3\cdot137$
659^2	$13\cdot33457$	739^2	$3\cdot7\cdot26041$	821^2	$7\cdot229\cdot421$
659^3	$2^3\cdot3\cdot5\cdot11\cdot17\cdot53\cdot241$	739^3	$2^3\cdot5\cdot37\cdot273061$	821^3	$2^2\cdot3\cdot137\cdot337021$

Num.	Summa divisorum	Num.	Summa divisorum	Num.	Summa divisorum
823	$2^3 \cdot 103$	881	$2 \cdot 3^2 \cdot 7^2$	947	$2^2 \cdot 3 \cdot 79$
823^2	$3 \cdot 7 \cdot 43 \cdot 751$	881^2	$19 \cdot 40897$	947^2	$7 \cdot 277 \cdot 463$
823^3	$2^4 \cdot 5 \cdot 103 \cdot 67733$	881^3	$2^2 \cdot 3^2 \cdot 7^2 \cdot 388081$	947^3	$2^3 \cdot 3 \cdot 5 \cdot 79 \cdot 89681$
827	$2^2 \cdot 3^2 \cdot 23$	883	$2^2 \cdot 13 \cdot 17$	953	$2 \cdot 3^2 \cdot 53$
827^2	684757	883^2	$3 \cdot 260191$	953^2	$181 \cdot 5023$
827^3	$2^3 \cdot 3^2 \cdot 5 \cdot 13 \cdot 23 \cdot 5261$	883^3	$2^3 \cdot 5 \cdot 13 \cdot 17 \cdot 77969$	953^3	$2^2 \cdot 3^2 \cdot 5 \cdot 53 \cdot 90821$
829	$2 \cdot 5 \cdot 83$	887	$2^3 \cdot 3 \cdot 37$	967	$2^3 \cdot 11^2$
829^2	$3 \cdot 211 \cdot 1087$	887^2	$13 \cdot 60589$	967^2	$3 \cdot 67 \cdot 4657$
829^3	$2^2 \cdot 5 \cdot 17^2 \cdot 29 \cdot 41 \cdot 83$	887^3	$2^4 \cdot 3 \cdot 5 \cdot 29 \cdot 37 \cdot 2713$	967^3	$2^4 \cdot 5 \cdot 11^2 \cdot 13 \cdot 7193$
839	$2^3 \cdot 3 \cdot 5 \cdot 7$	907	$2^2 \cdot 227$	971	$2^2 \cdot 3^5$
839^2	704761	907^2	$3 \cdot 7 \cdot 39217$	971^2	$13 \cdot 79 \cdot 919$
839^3	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 109 \cdot 3229$	907^3	$2^3 \cdot 5^2 \cdot 227 \cdot 16453$	971^3	$2^3 \cdot 3^5 \cdot 197 \cdot 2393$
853	$2 \cdot 7 \cdot 61$	911	$2^4 \cdot 3 \cdot 19$	977	$2 \cdot 3 \cdot 163$
853^2	$3 \cdot 43 \cdot 5647$	911^2	830833	977^2	$7 \cdot 136501$
853^3	$2^2 \cdot 5 \cdot 7 \cdot 13 \cdot 29 \cdot 61 \cdot 193$	911^3	$2^5 \cdot 3 \cdot 19 \cdot 29 \cdot 41 \cdot 349$	977^3	$2^2 \cdot 3 \cdot 5 \cdot 53 \cdot 163 \cdot 1801$
857	$2 \cdot 3 \cdot 11 \cdot 13$	919	$2^3 \cdot 5 \cdot 23$	983	$2^3 \cdot 3 \cdot 41$
857^2	735307	919^2	$3 \cdot 7 \cdot 13 \cdot 19 \cdot 163$	983^2	$103 \cdot 9391$
857^3	$2^2 \cdot 3 \cdot 5^2 \cdot 11 \cdot 13 \cdot 37 \cdot 397$	919^3	$2^4 \cdot 5 \cdot 23 \cdot 37 \cdot 101 \cdot 113$	983^3	$2^4 \cdot 3 \cdot 5 \cdot 13 \cdot 41 \cdot 7433$
859	$2^2 \cdot 5 \cdot 43$	929	$2 \cdot 3 \cdot 5 \cdot 31$	991	$2^5 \cdot 31$
859^2	$3 \cdot 246247$	929^2	$157 \cdot 5503$	991^2	$3 \cdot 7 \cdot 13^2 \cdot 277$
859^3	$2^3 \cdot 5 \cdot 43 \cdot 137 \cdot 2693$	929^3	$2^2 \cdot 3 \cdot 5 \cdot 31 \cdot 431521$	991^3	$2^6 \cdot 31 \cdot 491041$
863	$2^5 \cdot 3^3$	937	$2 \cdot 7 \cdot 67$	997	$2 \cdot 499$
863^2	$7^2 \cdot 15217$	937^2	$3 \cdot 292969$	997^2	$3 \cdot 13 \cdot 31 \cdot 823$
863^3	$2^6 \cdot 3^3 \cdot 5 \cdot 13 \cdot 17 \cdot 337$	937^3	$2^2 \cdot 5 \cdot 7 \cdot 67 \cdot 87797$	997^3	$2^2 \cdot 5 \cdot 499 \cdot 99401$
877	$2 \cdot 439$	941	$2 \cdot 3 \cdot 157$		
877^2	$3 \cdot 7 \cdot 37 \cdot 991$	941^2	$811 \cdot 1093$		
877^3	$2^2 \cdot 5 \cdot 439 \cdot 76913$	941^3	$2^2 \cdot 3 \cdot 13 \cdot 157 \cdot 34057$		

SCHOLION

14. Usus huius tabulae est amplissimus in quaestionibus circa divisores et partes aliquotas versantibus resolvendis. Eius enim ope cuiusque numeri propositi summa divisorum facili negotio inveniri potest; qua reperta si inde

ipse numerus propositus auferatur, remanebit eius summa partium aliquotarum. Ex quo statim constat huius tabulae subsidio numeros amicabiles, quos sum traditurus, facile explorari posse, utrum sint iusti necne. Quemadmodum autem ope huius tabulae cuiusvis numeri summa divisorum cognosci possit, in sequenti lemmate explicabo.

LEMMA 3

15. *Proposito quocunque numero eius summa divisorum sequenti modo colligitur.*

Cum omnis numerus sit vel primus vel productum ex primis, resolvatur numerus propositus in suos factores primos et, qui inter se fuerint aequales, coniunctim exprimantur. Hoc modo numerus propositus semper ad huiusmodi formam redigetur $m^\alpha \cdot n^\beta \cdot p^\gamma \cdot q^\delta \cdot$ etc. existentibus m, n, p, q etc. numeris primis. Posito ergo numero proposito $= N$ cum sit $N = m^\alpha \cdot n^\beta \cdot p^\gamma \cdot q^\delta \cdot$ etc. et factores m^α, n^β, p^γ, q^δ etc. inter se primi, erit $\int N = \int m^\alpha \cdot \int n^\beta \cdot \int p^\gamma \cdot \int q^\delta \cdot$ etc. et valores $\int m^\alpha$, $\int n^\beta$, $\int p^\gamma$, $\int q^\delta$ etc. ex tabula adiuncta patebunt.

EXEMPLUM 1

Sit numerus propositus $N = 360$.

Resoluto hoc numero in suos factores primos erit $N = 2^3 \cdot 3^2 \cdot 5$ ideoque

$$\int 360 = \int 2^3 \cdot \int 3^2 \cdot \int 5 = 3 \cdot 5 \cdot 13 \cdot 2 \cdot 3$$

ob $\int 2^3 = 3 \cdot 5$, $\int 3^2 = 13$, $\int 5 = 2 \cdot 3$. Unde his factoribus ordinatis fiet

$$\int 360 = 2 \cdot 3^2 \cdot 5 \cdot 13 = 1170.$$

EXEMPLUM 2

Explorentur numeri 2620 *et* 2924, *utrum sint amicabiles necne.*

Cum sit $2620 = 2^2 \cdot 5 \cdot 131$ et $2924 = 2^2 \cdot 17 \cdot 43$, examen ita instituetur.

Numeri propositi	2620	2924
per factores expressi	$2^2 \cdot 5 \cdot 131$	$2^2 \cdot 17 \cdot 43$
summae divisorum	$7 \cdot 6 \cdot 132$	$7 \cdot 18 \cdot 44$
sive	5544	5544
summae partium aliquotarum	2924	2620

Cum igitur summae partium aliquotarum sint numeris reciproce aequales, patet propositos numeros esse amicabiles.

SCHOLION

16. His igitur praemissis, quae ad inventionem divisorum cuiusque numeri pertinent, ipsum problema de investigatione numerorum amicabilium aggrediar atque scrutabor, quemadmodum huiusmodi numeros ratione summae divisorum inter se comparatos esse oporteat, quo deinceps facilius eorum inventio per regulas post tradendas suscipi queat.

PROBLEMA GENERALE

17. *Invenire numeros amicabiles, hoc est duos numeros huius indolis, ut alter aequalis sit summae partium aliquotarum alterius.*

SOLUTIO

Sint m et n duo huiusmodi numeri amicabiles et per hypothesin $\int m$ et $\int n$ summae divisorum eorundem. Erit numeri m summa partium aliquotarum $= \int m - m$ et numeri n summa partium aliquotarum $= \int n - n$. Hinc ex natura numerorum amicabilium nascentur hae duae aequationes

$$\int m - m = n \quad \text{et} \quad \int n - n = m$$

sive

$$\int m = \int n = m + n.$$

Numeri ergo amicabiles m et n primo habere debent eandem summam divisorum, tum vero oportet, ut haec communis divisorum summa aequalis sit aggregato ipsorum numerorum $m + n$.

COROLLARIUM 1

18. Problema ergo huc reducitur, ut quaerantur duo eiusmodi numeri, qui habeant eandem divisorum summam haecque aequalis sit aggregato ipsorum numerorum.

COROLLARIUM 2

19. Ipsa quidem problematis ratio exigit, ut bini numeri quaesiti sint inter se inaequales. Sin autem desiderentur aequales, ut sit $m=n$, fiet $\int n = 2n$ et $\int n - n = n$; huius scilicet numeri geminati n summa partium aliquotarum ipsi fiet aequalis, quae est proprietas numeri perfecti. Ergo quilibet numerus perfectus repetitus numeros exhibet amicabiles.

COROLLARIUM 3

20. Sin autem numeri amicabiles m et n, ut natura quaestionis postulat, sint inaequales, manifestum est alterum esse redundantem, alterum deficientem; summa scilicet partium aliquotarum alterius ipso erit maior, alterius vero ipso minor.

SCHOLION

21. Ex hac quidem generali proprietate parum adiumenti consequimur ad numeros amicabiles inveniendos, eo quod ista Analyseos species, cuius ope aequationem $\int m = \int n = m + n$ evolvere liceat, etiamnunc penitus sit inculta. Ob quem defectum formulas magis particulares contemplari cogimur, ex quarum indole regulas speciales pro inventione numerorum amicabilium derivare liceat; quorsum etiam pertinet regula CARTESIANA a SCHOTENIO commemorata[1]). Ac primo quidem, etiamsi non constet, utrum dentur numeri amicabiles inter se primi necne, formulas generales ita restringam, ut numeri amicabiles factorem communem obtineant.

1) Vide Commentationem 100 huius voluminis. F. R.

PROBLEMA PARTICULARE

22. *Invenire indolem numerorum amicabilium, qui communem habeant factorem.*

SOLUTIO

Sit a communis factor numerorum amicabilium, quorum alter ponatur $= am$, alter $= an$; sint vero tam m et a quam n et a numeri inter se primi, ut utriusque divisorum summa per praecepta data reperiri queat. Cum igitur primo utriusque eadem esse debeat divisorum summa, fiet $\int a \cdot \int m = \int a \cdot \int n$ ideoque

$$\int m = \int n.$$

Deinde vero necesse est, ut sit $\int a \cdot \int m$ seu $\int a \cdot \int n$ ipsorum numerorum aequalis aggregato $am + an$, unde habetur

$$\frac{a}{\int a} = \frac{\int m}{m+n} = \frac{\int n}{m+n}.$$

Positis ergo numeris amicabilibus am et an primo esse oportet $\int m = \int n$, tum vero requiritur, ut sit $a(m+n) = \int a \cdot \int m$.

COROLLARIUM 1

23. Si ergo pro m et n eiusmodi numeri iam fuerint eruti, ut sit $\int m = \int n$, tum numerus a investigari debet, ut sit $\frac{a}{\int a} = \frac{\int m}{m+n}$, seu ex ratione, quam numerus ad summam divisorum suorum tenere debet, ipse numerus a erit investigandus.

COROLLARIUM 2

24. Si factor communis a fuerit datus, quaestio ad inventionem numerorum m et n reducitur, qui prouti vel primi vel compositi ex duobus pluribusve primis assumuntur; quoniam tum divisorum summae actu exhiberi possunt, regulae speciales ad eos inveniendos tradi poterunt.

COROLLARIUM 3

25. Statim autem perspicitur utrumque numerum m et n primum esse non posse; quare casus simplicissimus extat, si alter primus, alter vero productum ex duobus numeris primis assumatur. Tum uterque productum ex duobus pluribusve numeris primis statui poterit, unde innumerae regulae speciales pro inveniendis numeris amicabilibus derivari poterunt.

SCHOLION

26. Diversae ergo numerorum amicabilium formae, quae hinc nascuntur, sequenti modo repraesentari poterunt. Sit a utriusque communis factor et p, q, r, s etc. numeri primi, quorum nullus sit divisor communis factoris a, atque numerorum amicabilium formae erunt:

$$\text{forma prima} \begin{cases} apq \\ ar \end{cases} \qquad \text{forma secunda} \begin{cases} apq \\ ars \end{cases}$$

$$\text{forma tertia} \begin{cases} apqr \\ as \end{cases} \qquad \text{forma quarta} \begin{cases} apqr \\ ast \end{cases} \qquad \text{forma quinta} \begin{cases} apqr \\ astu \end{cases}$$

etc.

Quanquam numerus harum formarum in infinitum augeri potest, minime tamen hinc concludere licet in his formis omnes numeros amicabiles contineri. Primum enim, dum hic litterae p, q, r, s, t etc. numeros primos diversos significant, non verisimile est nullos dari numeros amicabiles, in quibus non occurrant potestates eiusdem numeri primi. Deinde pariter non constat, utrum non dentur numeri amicabiles, qui vel nullum habeant factorem communem a, vel in quibus factor hic non prorsus sit idem, veluti si darentur numeri amicabiles huius formae $m^{\alpha}P$ et $m^{\beta}Q$, in quibus exponentes α et β essent diversi, quae forma propterea in superioribus non contineretur, etiamsi P et Q essent producta ex meris numeris primis inter se diversis.[1]) Ex his perspicitur quaestionem de numeris amicabilibus latissime patere eamque ob hoc ipsum tam esse difficilem, ut solutio completa vix sit expectanda. Solutionibus igitur particularibus equidem tantum incumbam et varias methodos aperiam, quarum ope ex formulis traditis plures numeros amicabiles mihi elicere licuit. Quaelibet autem forma duplicem mihi suppeditavit methodum, prout factor communis a vel datus assumitur vel ipse quaeritur; hasque methodos in sequentibus problematibus exponam.

1) Sed vide paria LX et LXI p. 162. F. R.

PROBLEMA 1

27. *Invenire numeros amicabiles primae formae apq et ar, si factor communis a sit datus.*

SOLUTIO

Cum p, q et r sint numeri primi atque $\int r = \int p \cdot \int q$ seu

$$r + 1 = (p + 1)(q + 1),$$

ponatur $p + 1 = x$ et $q + 1 = y$ fietque $r = xy - 1$. Ideoque x et y eiusmodi esse oportet numeros, ut tam $x - 1$ et $y - 1$ quam $xy - 1$ sint numeri primi. Deinde ut $a(x-1)(y-1)$ et $a(xy-1)$ sint numeri amicabiles, oportet, ut eorum aggregatum $a(2xy - x - y)$ aequale sit summae divisorum alterutrius $xy \int a$; unde nanciscimur hanc aequationem

$$xy \int a = 2axy - ax - ay \quad \text{seu} \quad y = \frac{ax}{(2a - \int a)x - a}.$$

Sit brevitatis gratia $\frac{a}{2a - \int a} = \frac{b}{c}$ et $\frac{b}{c}$ sit valor fractionis $\frac{a}{2a - \int a}$ ad minimos terminos reductae eritque

$$y = \frac{bx}{cx - b} \quad \text{seu} \quad cy = \frac{bcx}{cx - b} = b + \frac{bb}{cx - b},$$

unde habebimus

$$(cx - b)(cy - b) = bb.$$

Cum igitur $cx - b$ et $cy - b$ sint factores ipsius bb, quadratum cognitum bb in eiusmodi binos factores resolvi debet, quorum uterque numero b auctus fiat per c divisibilis et quoti x et y inde emergentes ita sint comparati, ut $x - 1$, $y - 1$ et $xy - 1$ evadant numeri primi. Quae conditio quoties obtineri poterit, quod quidem pro quovis valore ipsius a assumto statim dispicitur, toties obtinebuntur numeri amicabiles, qui erunt $a(x-1)(y-1)$ et $a(xy-1)$.

COROLLARIUM

28. Prout igitur pro a alii aliique numeri accipiuntur, unde valores b et c innotescant, regulae emergent particulares, quarum ope numeri amicabiles, si qui in eo genere dantur, facile eruentur.

REGULA 1

29. Sit factor communis a potestas quaecunque binarii, puta $a = 2^n$; erit $\int a = 2^{n+1} - 1$ ideoque $2a - \int a = 1$, unde erit $\frac{a}{2a - \int a} = 2^n$ et propterea $b = 2^n$ et $c = 1$. Hinc oritur

$$(x - 2^n)(y - 2^n) = 2^{2n}.$$

Quare cum 2^{2n} alios non habeat factores nisi potestates binarii, erit

$$x - 2^n = 2^{n+k}, \quad y - 2^n = 2^{n-k}$$

seu

$$x = 2^{n+k} + 2^n, \quad y = 2^{n-k} + 2^n.$$

Quocirca dispiciendum est, an eiusmodi valor pro k detur, ut sequentes tres numeri

$$x - 1 = 2^{n+k} + 2^n - 1, \quad y - 1 = 2^{n-k} + 2^n - 1,$$

$$xy - 1 = 2^{2n+1} + 2^{2n+k} + 2^{2n-k} - 1$$

fiant numeri primi. Quod si succedat, erunt numeri amicabiles

$$2^n(2^{n+k} + 2^n - 1)(2^{n-k} + 2^n - 1), \quad 2^n(2^{2n+1} + 2^{2n+k} + 2^{2n-k} - 1).$$

Vel sit $n - k = m$ seu $n = m + k$ fietque

$$x - 1 = 2^m(2^{2k} + 2^k) - 1 = q, \quad y - 1 = 2^m(1 + 2^k) - 1 = p,$$

$$xy - 1 = 2^{2m}(2^{2k+1} + 2^{3k} + 2^k) - 1 = r,$$

qui numeri, quoties fuerint primi, praebebunt numeros amicabiles.

CASUS 1

30. Sit $k = 1$ et numeri amicabiles obtinebuntur, quoties sequentes tres numeri fuerint primi

$$3 \cdot 2^m - 1, \quad 6 \cdot 2^m - 1 \quad \text{et} \quad 18 \cdot 2^{2m} - 1.$$

Tum enim positis

$$p = 3 \cdot 2^m - 1, \quad q = 6 \cdot 2^m - 1 \quad \text{et} \quad r = 18 \cdot 2^{2m} - 1$$

numeri amicabiles erunt

$$2^{m+1}pq \quad \text{et} \quad 2^{m+1}r$$

ob $n = m + k = m + 1$. Haecque est regula CARTESII a SCHOTENIO tradita.[1])

EXEMPLUM 1

31. Sit $m = 1$ eritque

$$p = 3 \cdot 2 - 1 = 5 \quad \text{numerus primus,}$$
$$q = 6 \cdot 2 - 1 = 11 \quad \text{numerus primus,}$$
$$r = 18 \cdot 4 - 1 = 71 \quad \text{numerus primus.}$$

Hinc ergo oriuntur numeri amicabiles

$$2^2 \cdot 5 \cdot 11 \quad \text{et} \quad 2^2 \cdot 71 \quad \text{sive} \quad 220 \quad \text{et} \quad 284,$$

qui sunt minimi omnium, qui exhiberi possunt.

EXEMPLUM 2

32. Sit $m = 2$ eritque $2^m = 4$ et $2^{2m} = 16$ atque

$$p = 3 \cdot 4 - 1 = 11 \quad \text{numerus primus,}$$
$$q = 6 \cdot 4 - 1 = 23 \quad \text{numerus primus,}$$
$$r = 18 \cdot 16 - 1 = 287 \quad \text{numerus non-primus;}$$

hincque adeo nulli numeri amicabiles oriuntur.

EXEMPLUM 3

33. Sit $m = 3$ eritque $2^m = 8$ et $2^{2m} = 64$ atque

$$p = 3 \cdot 8 - 1 = 23 \quad \text{primus,}$$
$$q = 6 \cdot 8 - 1 = 47 \quad \text{primus,}$$
$$r = 18 \cdot 64 - 1 = 1151 \quad \text{primus.}$$

Ergo hinc numeri amicabiles erunt

$$2^4 \cdot 23 \cdot 47 \quad \text{et} \quad 2^4 \cdot 1151 \quad \text{sive} \quad 17296 \quad \text{et} \quad 18416.$$

1) Vide Commentationem 100 huius voluminis. F. R.

EXEMPLA SEQUENTIA

34. Haec exempla cum sequentibus, in quibus exponenti m maiores valores tribuuntur, commodius uno conspectu ita repraesentari poterunt:

Sit $m = 1$	2	3	4	5	6	7	8
erit $p = 5$	11	23	47	95*	191	383	767*
$q = 11$	23	47	95*	191	383	767*	1535*
$r = 71$	287*	1151	4607*	18431*	73727	294911	1179647*

Ubi numeri non-primi asteriscis[1]) sunt notati; unde hinc tantum terni numeri amicabiles[2]) obtinentur, nempe

$$\text{I.} \begin{cases} 2^2 \cdot 5 \cdot 11 \\ 2^2 \cdot 71 \end{cases} \qquad \text{II.} \begin{cases} 2^4 \cdot 23 \cdot 47 \\ 2^4 \cdot 1151 \end{cases} \qquad \text{III.} \begin{cases} 2^7 \cdot 191 \cdot 383 \\ 2^7 \cdot 73727. \end{cases}$$

Ulterius autem progredi non licet, quoniam valores ipsius r nimis fiunt magni, quam ut dignosci possit, utrum sint primi necne. Tabulae namque numerorum primorum adhuc constructae[3]) vix ultra 100000 porriguntur.

---

1) Qui quidem in editione principe hic et in sequentibus tabulis nonnullis numeris non-primis desunt. F. R.

2) Qui numeri constituunt ista tria paria ante EULERUM cognita; vide notam 1 p. 60. F. R.

3) Vide J. W. L. GLAISHER (CAYLEY, STOKES, THOMSON, SMITH and GLAISHER), *Report on Mathematical Tables*, Brit. Assoc. Rep. XLIII, 1873, p. 1, imprimis p. 34—40. Inter libros hac in relatione enumeratos sequentes tres utpote ante a. 1750 editi digni sunt, qui hic commemorentur: 1) J. H. RAHN, *Teutsche Algebra*, Zürich 1659. Continet tabulam divisorum numerorum imparium usque ad 24000. — 2) Translatio huius insignis libri, quae inscribitur *An Introduction to Algebra, translated out of the High-Dutch into English by THOMAS BRANCKER. Much altered and augmented by D. P[ELL]*... London 1668. (Vide G. WERTHEIM, *Die Algebra des JOHANN HEINRICH RAHN (1659) und die englische Übersetzung derselben*, Biblioth. Mathem. 3_3, 1902, p. 113.) Qua in translatione J. PELL tabulam divisorum a RHONIO (= RAHN) constructam usque ad 100000 continuavit. Nonnullas (30) correctiones huius tabulae PELLIANAE dedit J. WALLIS in opere, quod inscribitur *A Treatise of Algebra*, Oxford 1685 (Addit. Treat. IV, p. 136). — 3) J. G. KRÜGER, *Gedanken von der Algebra*, Halle 1746. Continet tabulam numerorum primorum usque ad 100999, qua tabula sine dubio uti solebat EULERUS. Reperitur enim hoc opus in EULERI indice *Catalogus librorum meorum*, cuius mentionem facit G. ENESTRÖM in relatione *Bericht an die Eulerkommission der Schweizerischen Naturforschenden Gesellschaft über die EULERSCHEN Manuskripte der Petersburger Akademie*, Jahresber. d. Deutschen Mathem.-Ver. 22, 1913, p. 191; vide p. 197: „[*Sechstes Notizbuch*]... *S. 363—402 befindet sich ein Verzeichnis der Bibliothek LEONHARD EULERS* (539 Büchertitel)". F. R.

CASUS 2

35. Sit $k = 2$ et valores litterarum p, q, r, qui debent esse primi, erunt

$$p = 5 \cdot 2^m - 1, \quad q = 20 \cdot 2^m - 1, \quad r = 100 \cdot 2^{2m} - 1;$$

quorum cum postremus semper sit per ternarium divisibilis ob $2^{2m} = 3\alpha + 1$ et $r = 300\alpha + 99$, hinc nulli numeri amicabiles consequuntur.

CASUS 3

36. Ponatur $k = 3$ eritque

$$p = 9 \cdot 2^m - 1, \quad q = 72 \cdot 2^m - 1, \quad r = 648 \cdot 2^{2m} - 1;$$

quorum cum nullus necessario videatur divisorem admittere, valores ipsorum p, q, r ex valoribus simplicioribus ipsius m oriundos hic coniunctim repraesentabo:

$m =$	1	2	3	4	5
$p =$	17	35*	71	143*	287*
$q =$	143*	287*	575*	1151	2303*
$r =$	2591	10367*	41471*	165887	663551*

Hinc ergo, quoniam ulterius progredi non licet, nulli numeri amicabiles inveniuntur.

CASUS 4

37. Ponatur $k = 4$ et sequentes tres numeri debebunt esse primi

$$p = 17 \cdot 2^m - 1, \quad q = 272 \cdot 2^m - 1, \quad r = 4624 \cdot 2^{2m} - 1.$$

Ubi cum r semper sit multiplum ternarii, patet hinc nullos prodire numeros amicabiles.

CASUS 5

38. Ponatur $k = 5$ et sequentes tres numeri debebunt esse primi

$$p = 33 \cdot 2^m - 1, \quad q = 1056 \cdot 2^m - 1, \quad r = 34848 \cdot 2^{2m} - 1.$$

Ubi statim patet casum $m = 1$ esse inutilem, cum det $p = 65$. Sit ergo $m = 2$ fietque $p = 131$, $q = 4223$*, $r = 557567$; ubi cum q non sit primus et maiores valores pro m ob defectum tabularum numerorum primorum examini subiici nequeant, neque hinc etiam novi numeri amicabiles eruuntur. At vero ob eandem rationem maiores valores ipsi k tribuere non licet.

SCHOLION

39. Quoniam potestates binarii pro a positae valorem ipsius c in fractione $\frac{b}{c} = \frac{a}{2a - \int a}$ unitati aequalem reddiderunt hincque solutiones obtinere licuit, alios valores pro a, qui pariter ipsi c valorem $= 1$ inducant, ponam. Inter hos autem imprimis sunt notandi, qui ex hac forma $a = 2^n(2^{n+1} + e)$ nascuntur, siquidem $2^{n+1} + e$ sit numerus primus; tum enim fit

$$2a - \int a = e + 1 \quad \text{et} \quad \frac{b}{c} = \frac{2^n(2^{n+1} + e)}{e + 1};$$

si igitur $e + 1$ sit divisor numeratoris $2^n(2^{n+1} + e)$, valor ipsius c fiet itidem $= 1$.

REGULA 2

40. Sit factor communis $a = 2^n(2^{n+1} + 2^k - 1)$, at $2^{n+1} + 2^k - 1$ numerus primus; erit ob $e + 1 = 2^k$ fractio $\frac{b}{c} = \frac{2^n(2^{n+1} + 2^k - 1)}{2^k} = 2^{n-k}(2^{n+1} + 2^k - 1)$, siquidem non sit $k > n$. Hac ergo hypothesi habebimus

$$b = 2^{n-k}(2^{n+1} + 2^k - 1) \quad \text{et} \quad c = 1.$$

Quadratum ergo bb in duos eiusmodi factores $(x - b)(y - b)$ resolvendum est, ex quibus non solum valores numerorum $x - 1 = p$ et $y - 1 = q$, sed etiam $xy - 1 = r$ fiant numeri primi. Cuiusmodi casus si eruere liceat, erunt numeri amicabiles apq et ar. Verum hic notandum est eos casus reiiciendos esse, in quibus aliquis numerorum primorum p, q, r prodit divisor ipsius a seu aequalis $2^{n+1} + 2^k - 1$, quia a per nullum alium numerum primum est divisibile.

Sit $n - k = m$ seu $n = m + k$; erit

$$a = 2^{m+k}(2^{m+k+1} + 2^k - 1) \quad \text{et} \quad b = 2^m(2^{m+k+1} + 2^k - 1).$$

Iam quia $2^{m+k+1}+2^k-1$ debet esse numerus primus, ponatur

$$2^{m+k+1}+2^k-1=f \quad \text{seu} \quad f=2^k(2^{m+1}+1)-1,$$

ut sit

$$a=2^{m+k}f \quad \text{et} \quad b=2^m f;$$

erit

$$bb=2^{2m}ff=(x-b)(y-b).$$

Nunc ob f numerum primum numerus $2^{2m}ff$ duplici modo in genere in duos factores resolvetur.

Priori modo fiet

$$(x-b)(y-b)=2^{m-\alpha}f\cdot 2^{m+\alpha}f$$

ideoque

$$x=2^{m-\alpha}f+2^m f, \qquad y=2^{m+\alpha}f+2^m f,$$

et

$$p=(2^{m-\alpha}+2^m)f-1, \qquad q=(2^{m+\alpha}+2^m)f-1$$

$$r=(2^{2m+1}+2^{2m+\alpha}+2^{2m-\alpha})ff-1,$$

qui tres numeri p, q, r debent esse primi.

Posteriori modo resolutio fiet ita

$$(x-b)(y-b)=2^{m\pm\alpha}\cdot 2^{m\mp\alpha}ff,$$

unde fit

$$x=2^{m\pm\alpha}+2^m f, \qquad y=2^{m\mp\alpha}ff+2^m f,$$

et

$$p=2^{m\pm\alpha}+2^m f-1, \qquad q=(2^{m\mp\alpha}f+2^m)f-1$$

$$r=(2^{2m+1}f+2^{2m\pm\alpha}+2^{2m\mp\alpha}ff)f-1,$$

et quoties p, q, r hoc modo prodeunt numeri primi, inde oriuntur numeri amicabiles apq et ar.

CASUS 1

41. Sit $k=1$; erit $a=2^{m+1}(2^{m+2}+1)$, $b=2^m(2^{m+2}+1)$ atque $f=2^{m+2}+1$, qui numerus debet esse primus. Cum ergo sit $(x-b)(y-b)=2^{2m}ff$, erit

vel

$$p=(2^{m-\alpha}+2^m)f-1,$$
$$q=(2^{m+\alpha}+2^m)f-1,$$
$$r=(2^{2m+1}+2^{2m+\alpha}+2^{2m-\alpha})ff-1$$

vel

$$p=2^{m\pm\alpha}+2^m f-1,$$
$$q=(2^{m\mp\alpha}f+2^m)f-1,$$
$$r=(2^{2m+1}f+2^{2m\pm\alpha}+2^{2m\mp\alpha}ff)f-1.$$

Notandum autem est, ut $2^{m+2}+1$ sit numerus primus, exponentem $m+2$ esse oportere potestatem binarii; valores ergo ipsius m erunt 0, 2, 6, 14 etc. At casus $m=0$ reiici debet ob nullum valorem ipsius α assignabilem.

EXEMPLUM 1

42. Sit ergo $m=2$, ut sit $a=8\cdot 17$ et $b=4\cdot 17=68$ atque $f=17$. Cum igitur esse debeat $(x-b)(y-b)=4^2\cdot 17^2$, erit resolutione in factores instituenda:

$x-68=$	2	4	8	34
$y-68=$	$8\cdot 17^2$	1156	578	136
$x=$	70	72	76	102
$y=$	2380	1224	646	204
$p=$	69*	71	75*	101
$q=$	2379*	1223	645*	203*
$r=$	166599*	88127*	49095*	20807

Hinc ergo nulli numeri amicabiles obtinentur.

EXEMPLUM 2

43. Sit $m=6$, ut $a=2^7\cdot 257$, $b=2^6\cdot 257$ et $f=257$. Cum igitur sit $(x-b)(y-b)=2^{12}\cdot 257^2$, resolutio ita institui debebit:

$x-16448=$	$32\cdot 257$
$y-16448=$	$128\cdot 257$
$x=$	24672
$y=$	49344
$p=$	24671
$q=$	49343*
$r=$	. . .

Valores ex reliquis factoribus oriundi adhuc magis fiunt magni, quam ut, an primi sint necne, iudicari possit.

CASUS RELIQUI

44. Cum $f = 2^{m+k+1} + 2^k - 1$ debeat esse numerus primus, quaeramus primo casus simpliciores, quibus hoc evenit, cum casus nimis compositos evolvere non liceat. Sit ergo $k = 2$ et ob $f = 2^{m+3} + 3$ valores idonei pro m erunt 1, 3, 4. Sit $k = 3$; erit $f = 2^{m+4} + 7$ et valores idonei pro m erunt 2, 4, 6. Casu $k = 4$ est $f = 2^{m+5} + 15$ et m erit 1 vel 3; neque ulterius progredi licet.

EXEMPLUM 1

45. Ponamus ergo $k = 2$ et $m = 1$; erit $f = 19$ et $a = 8 \cdot 19$ atque $b = 2 \cdot 19 = 38$, unde fiet $(x - 38)(y - 38) = 2^2 \cdot 19^2 = 1444$, et resolutio dabit:

$x - 38 =$	2	4	Neuter scilicet factor assumi potest impar.
$y - 38 =$	722	361	
$x =$	40		
$y =$	760	imp.	
$p =$	39*		

Quia hic iam p non est primus, patet hinc nullos numeros amicabiles resultare.

EXEMPLUM 2

46. Ponamus $k = 2$ et $m = 3$, ut sit $f = 67$; erit $a = 32 \cdot 67$ et $b = 8 \cdot 67 = 536$, unde fit $(x - 536)(y - 536) = 2^6 \cdot 67^2$.

$x - 536 =$	268	16	Reliqui valores pro p praebent numeros per 3 divisibiles, quos propterea omisi. Sequentia exempla ad nimis magnos numeros deducunt.
$y - 536 =$	1072	17956	
$x =$	804	552	
$y =$	1608	. . .	
$p =$	803*	551*	
$q =$	1607	. . .	

REGULA 3

47. Sit ut ante $a = 2^n(2^{n+1} + 2^k - 1)$ et $2^{n+1} + 2^k - 1 = f$ numerus primus, at in fractione $\frac{b}{c} = \frac{2^n(2^{n+1}+2^k-1)}{2^k}$ sit $k > n$ eritque

$$b = 2^{n+1} + 2^k - 1 \quad \text{et} \quad c = 2^{k-n}.$$

Ponamus $k - n = m$, ut sit $k = m + n$; erit

$$a = 2^n(2^{n+1} + 2^{m+n} - 1), \quad b = 2^{n+1} + 2^{m+n} - 1 = f \quad \text{et} \ c = 2^m,$$

unde haec habebitur aequatio

$$(2^m x - b)(2^m y - b) = bb.$$

Cum autem $b = f$ sit numerus primus, alia resolutio locum non invenit praeter $1 \cdot bb$, ex qua fit

$$x = \frac{1+b}{2^m} \quad \text{et} \quad y = \frac{b(1+b)}{2^m}$$

sive

$$x = 2^n + 2^{n+1-m} \quad \text{et} \quad y = (2^{n+1} + 2^{m+n} - 1)(2^n + 2^{n+1-m}).$$

Iam notandum est hos quatuor numeros esse oportere primos

$$f = 2^{n+1} + 2^{m+n} - 1, \quad p = x - 1, \quad q = y - 1 \quad \text{et} \quad r = xy - 1$$

atque necesse est, ut sit $m < n + 1$. Quibus conditionibus si satisfiat, erunt numeri amicabiles apq et ar.

CASUS 1

48. Sit $m = 1$; erit $f = 2^{n+2} - 1$, $x = 2^{n+1}$ et $p = 2^{n+1} - 1$; fieri autem nequit, ut simul et f et p sit numerus primus nisi casu $n = 1$, quo vero fit $q = 27$. Ergo ex hypothesi $m = 1$ nulli oriuntur numeri amicabiles.

CASUS 2

49. Sit ergo $m = 2$, ut sit

$$f = 3 \cdot 2^{n+1} - 1, \quad x = 3 \cdot 2^{n-1} \quad \text{et} \quad y = 3 \cdot 2^{n-1}(3 \cdot 2^{n+1} - 1) \quad \text{atque} \quad a = 2^n \cdot f.$$

Sequentes ergo quatuor numeri debent esse primi

$$f=3\cdot 2^{n+1}-1,\quad p=3\cdot 2^{n-1}-1,\quad q=3\cdot 2^{n-1}(3\cdot 2^{n+1}-1)-1$$

et

$$r=9\cdot 2^{2n-2}(3\cdot 2^{n+1}-1)-1,$$

unde formantur haec exempla:

$n=$	1	2	3	4	5
$f=$	11	23	47	95*	191
$p=$	2	5	11	. . .	47
$q=$	32*	137	563	. . .	9167*
$r=$	98*	827	6767*	. . .	. . .

hincque ergo ex $n=2$ et $a=4\cdot 23$ nascuntur numeri amicabiles

$$\begin{cases}4\cdot 23\cdot 5\cdot 137\\ 4\cdot 23\cdot 827.\end{cases}$$

CASUS CETERI

50. Si $m=3$, iterum vel f vel p fit divisibile per 3, quod idem evenit, si $m=5$ vel 7 etc. Sit ergo $m=4$; erit

$$f=9\cdot 2^{n+1}-1,\quad x=9\cdot 2^{n-3}\quad\text{et}\quad y=9\cdot 2^{n-3}(9\cdot 2^{n+1}-1)\quad\text{et}\quad a=2^n\cdot f,$$

unde formantur haec exempla:

$n=$	1	4	5	6
$f=$	35*	287*	575*	1151
$x=$	. . .	. . .	. . .	72
$y=$	. . .	. . .	. . .	82872
$p=$	. . .	. . .	. . .	71
$q=$	. . .	. . .	. . .	82871*
$r=$	. . .	. . .	. . .	. . .

Neque ergo hinc neque ex maioribus valoribus ipsi m tribuendis numeros amicabiles elicere licet.

REGULA 4

51. Possunt etiam aliae expressiones pro factore communi a inveniri, ex quibus fractionis $\frac{b}{c}$ denominator c vel unitati vel potestati binarii fiat aequalis. Fingamus namque $a = 2^n(g-1)(h-1)$, ut sint $g-1$ et $h-1$ numeri primi; erit

$$\int a = (2^{n+1}-1)gh = 2^{n+1}gh - gh;$$

at est $2a = 2^{n+1}gh - 2^{n+1}g - 2^{n+1}h + 2^{n+1}$, unde fit

$$2a - \int a = gh - 2^{n+1}g - 2^{n+1}h + 2^{n+1}.$$

Ponatur $2a - \int a = d$; erit $gh - 2^{n+1}(g+h) + 2^{n+1} = d$ et

$$(g - 2^{n+1})(h - 2^{n+1}) = d - 2^{n+1} + 2^{2n+2},$$

unde per resolutionem in factores eiusmodi valores pro g et h elici debent, ut $g-1$ et $h-1$ fiant numeri primi; eritque tum

$$a = 2^n(g-1)(h-1) \quad \text{et} \quad \frac{b}{c} = \frac{a}{d}.$$

I. Ponamus $n = 1$; erit

$$(g-4)(h-4) = d + 12;$$

ubi ut $d + 12$ duos obtineat factores pares, sequentes prodibunt valores:

Sit $d = 4$; erit

$$(g-4)(h-4) = 16 = 2 \cdot 8, \quad \text{unde} \quad g = 6, \quad h = 12,$$

$$a = 2 \cdot 5 \cdot 11 \quad \text{atque} \quad \frac{b}{c} = \frac{2 \cdot 5 \cdot 11}{4}, \quad \text{ergo} \quad b = 5 \cdot 11 \quad \text{et} \quad c = 2.$$

Sit $d = 8$; erit

$$(g-4)(h-4) = 20 = 2 \cdot 10, \quad \text{unde} \quad g = 6, \quad h = 14,$$

$$a = 2 \cdot 5 \cdot 13 \quad \text{atque} \quad \frac{b}{c} = \frac{2 \cdot 5 \cdot 13}{8}, \quad \text{ergo} \quad b = 5 \cdot 13 \quad \text{et} \quad c = 4.$$

Sit $d = 16$; erit

$$(g-4)(h-4) = 28 = 2 \cdot 14, \quad \text{unde} \quad g = 6, \quad h = 18,$$

$$a = 2 \cdot 5 \cdot 17 \quad \text{atque} \quad \frac{b}{c} = \frac{2 \cdot 5 \cdot 17}{16}, \quad \text{ergo} \quad b = 5 \cdot 17 \quad \text{et} \quad c = 8.$$

II. Ponamus $n = 2$; erit

$$(g-8)(h-8) = d + 56$$

atque $a = 4(g-1)(h-1)$, unde sequentes casus resultant:

Sit $d = 4$; erit

$$(g-8)(h-8) = 60 = 6 \cdot 10, \quad \text{unde} \quad g = 14, \quad h = 18,$$

$$a = 4 \cdot 13 \cdot 17 \quad \text{atque} \quad \frac{b}{c} = \frac{4 \cdot 13 \cdot 17}{4}, \quad \text{ergo} \quad b = 13 \cdot 17 \quad \text{et} \quad c = 1.$$

Sit $d = 8$; erit

$$(g-8)(h-8) = 64 = 4 \cdot 16, \quad \text{unde} \quad g = 12, \quad h = 24,$$

$$a = 4 \cdot 11 \cdot 23 \quad \text{atque} \quad \frac{b}{c} = \frac{4 \cdot 11 \cdot 23}{8}, \quad \text{ergo} \quad b = 11 \cdot 23 \quad \text{et} \quad c = 2.$$

Sit $d = 16$; erit

$$(g-8)(h-8) = 72 = 6 \cdot 12, \quad \text{unde} \quad g = 14, \quad h = 20,$$

$$a = 4 \cdot 13 \cdot 19 \quad \text{atque} \quad \frac{b}{c} = \frac{4 \cdot 13 \cdot 19}{16}, \quad \text{ergo} \quad b = 13 \cdot 19 \quad \text{et} \quad c = 4.$$

III. Ponamus $n = 3$, ut sit $a = 8(g-1)(h-1)$, oportebitque esse

$$(g-16)(h-16) = d + 240.$$

Sit $d = 4$; erit

$$(g-16)(h-16) = 244 = 2 \cdot 122, \quad \text{unde} \quad g = 18, \quad h = 138,$$

$$a = 8 \cdot 17 \cdot 137 \quad \text{et} \quad \frac{b}{c} = \frac{8 \cdot 17 \cdot 137}{4}, \quad \text{ergo} \quad b = 2 \cdot 17 \cdot 137 \quad \text{et} \quad c = 1.$$

Sit $d=8$; erit

$$(g-16)(h-16)=248=2\cdot 124, \quad \text{unde} \quad g=18, \quad h=140,$$

$$a=8\cdot 17\cdot 139 \quad \text{et} \quad \frac{b}{c}=\frac{8\cdot 17\cdot 139}{8}, \quad \text{ergo} \quad b=17\cdot 139 \quad \text{et} \quad c=1.$$

Sit $d=16$; erit

$$(g-16)(h-16)=256=4\cdot 64, \quad \text{unde} \quad g=20, \quad h=80,$$

$$a=8\cdot 19\cdot 79 \quad \text{et} \quad \frac{b}{c}=\frac{8\cdot 19\cdot 79}{16}, \quad \text{ergo} \quad b=19\cdot 79 \quad \text{et} \quad c=2.$$

Sit iterum $d=16$ et

$$(g-16)(h-16)=8\cdot 32; \quad \text{unde} \quad g=24, \quad h=48,$$

$$a=8\cdot 23\cdot 47 \quad \text{et} \quad \frac{b}{c}=\frac{8\cdot 23\cdot 47}{16}, \quad \text{ergo} \quad b=23\cdot 47 \quad \text{et} \quad c=2.$$

Sumtis autem hinc valoribus pro a si numeri amicabiles statuantur $a(x-1)(y-1)$ et $a(xy-1)$, ut sint $x-1$, $y-1$ et $xy-1$ numeri primi, efficiendum est, ut sit $(cx-b)(cy-b)=bb$.

EXEMPLUM 1

52. Sit $a=2\cdot 5\cdot 11$; erit $b=5\cdot 11=55$ et $c=2$, unde fiet

$$(2x-55)(2y-55)=5^2\cdot 11^2.$$

$2x-55$	1	5	25
$2y-55$	3025	605	121
x	28	30	40
y	1540	330	88
$x-1$	27*	29	39*
$y-1$	. . .	329*	. . .
$xy-1$	. . .	. . .	. . .

Hinc ergo nulli obtinentur numeri amicabiles.

EXEMPLUM 2

53. Sit $a = 2 \cdot 5 \cdot 13$; erit $b = 5 \cdot 13 = 65$ et $c = 4$, unde fit

$$(4x - 65)(4y - 65) = 5^2 \cdot 13^2.$$

At hic numerus $5^2 \cdot 13^2$ non resolvi potest in duos factores, qui 65 aucti fiant per 4 divisibiles; quod idem in valore $a = 2 \cdot 5 \cdot 17$ usu venit.

EXEMPLUM 3

54. Sit $a = 4 \cdot 13 \cdot 17$; erit $b = 13 \cdot 17 = 221$ et $c = 1$ esseque oportet $(x - 221)(y - 221) = 13^2 \cdot 17^2$, unde

$x - 221$	13	17	169
$y - 221$	3757	. . .	289
$x - 1$	233	237*	389
$y - 1$	3977*	. . .	509
$xy - 1$	. . .	. . .	198899

In resolutione ultima fit $x - 1$ et $y - 1$ numerus primus, quaestio ergo huc redit, utrum $xy - 1 = 198899$ sit numerus primus necne. Etiamsi autem hic numerus terminum 100000 excedat, tamen demonstrare possum eum esse primum, unde numeri amicabiles erunt

$$\begin{cases} 4 \cdot 13 \cdot 17 \cdot 389 \cdot 509 \\ 4 \cdot 13 \cdot 17 \cdot 198899. \end{cases}$$

SCHOLION

55. Numerum autem hunc 198899 esse primum inde colligo, quod observavi esse $198899 = 2 \cdot 47^2 + 441^2$, ita ut 198899 sit numerus in hac forma $2aa + bb$ contentus. Certum autem est, si quis numerus unico modo in forma $2aa + bb$ contineatur, tum eum esse primum, sin autem duplici vel pluribus modis ad formam $2aa + bb$ redigi queat, tum esse compositum.[1]) Quaesivi ergo, utrum a numero hoc 198899 aliud quadratum duplum praeter

1) Vide Commentationem 256 huius voluminis, theorema 10. F. R.

47^2 subtrahi queat, ut residuum evadat quadratum, nullumque subducto calculo inveni; ex quo tuto conclusi hunc numerum esse primum ideoque numeros inventos esse amicabiles. Ex reliquis autem valoribus ipsius a, quos exhibui, nulli reperiuntur numeri amicabiles.

REGULA 5

56. Possunt etiam alii numeri idonei pro a assumi, ex quibus numeros amicabiles eruere liceat. Cum autem pro iis regula generalis tradi nequeat, aliquos tantum hic evolvam, ad quorum imitationem non erit difficile alios excogitare.

I. Sit ergo $a = 3^2 \cdot 5 \cdot 13$; erit $\int a = 13 \cdot 6 \cdot 14$ et ob $2a = 90 \cdot 13$ et $\int a = 84 \cdot 13$ erit $2a - \int a = 6 \cdot 13$ atque $\frac{b}{c} = \frac{a}{2a - \int a} = \frac{3^2 \cdot 5 \cdot 13}{6 \cdot 13} = \frac{15}{2}$ ideoque $b = 15$ et $c = 2$.

II. Sit $a = 3^2 \cdot 7 \cdot 13$; erit $\int a = 13 \cdot 8 \cdot 14 = 16 \cdot 7 \cdot 13$, unde ob $2a = 18 \cdot 7 \cdot 13$ erit $2a - \int a = 2 \cdot 7 \cdot 13$ ideoque $\frac{b}{c} = \frac{3^2 \cdot 7 \cdot 13}{2 \cdot 7 \cdot 13} = \frac{9}{2}$, unde $b = 9$ et $c = 2$.

III. Sit $a = 3^2 \cdot 7^2 \cdot 13$; erit $\int a = 13 \cdot 3 \cdot 19 \cdot 14 = 2 \cdot 3 \cdot 7 \cdot 13 \cdot 19$ et $2a = 42 \cdot 3 \cdot 7 \cdot 13$, unde $2a - \int a = 4 \cdot 3 \cdot 7 \cdot 13$ ideoque $\frac{b}{c} = \frac{3^2 \cdot 7^2 \cdot 13}{4 \cdot 3 \cdot 7 \cdot 13} = \frac{21}{4}$, ergo $b = 21$ et $c = 4$.

IV. Sit $a = 3^2 \cdot 5$; erit $\int a = 5 \cdot 8 \cdot 6 = 16 \cdot 3 \cdot 5$. Ergo ob $2a = 18 \cdot 3 \cdot 5$ erit $2a - \int a = 2 \cdot 3 \cdot 5$ hincque $\frac{b}{c} = \frac{3^2 \cdot 5}{2 \cdot 3 \cdot 5} = \frac{9}{2}$ et $b = 9$ et $c = 2$.

V. Sit $a = 3^2 \cdot 5 \cdot 13 \cdot 19$; erit $\int a = 13 \cdot 6 \cdot 14 \cdot 20 = 16 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ et ob $2a = 114 \cdot 3 \cdot 5 \cdot 13$ et $\int a = 112 \cdot 3 \cdot 5 \cdot 13$ erit $\frac{b}{c} = \frac{3^2 \cdot 5 \cdot 13 \cdot 19}{2 \cdot 3 \cdot 5 \cdot 13} = \frac{3 \cdot 19}{2}$ et $b = 3 \cdot 19 = 57$ et $c = 2$.

VI. Sit $a = 3^2 \cdot 7^2 \cdot 13 \cdot 19$; erit $\int a = 13 \cdot 3 \cdot 19 \cdot 14 \cdot 20 = 8 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19$ et ob $2a = 42 \cdot 3 \cdot 7 \cdot 13 \cdot 19$ erit $\frac{b}{c} = \frac{3^2 \cdot 7^2 \cdot 13 \cdot 19}{2 \cdot 3 \cdot 7 \cdot 13 \cdot 19} = \frac{21}{2}$, unde fit $b = 21$ et $c = 2$.

Positis autem numeris amicabilibus $a(x-1)(y-1)$ et $a(xy-1)$ fieri debet $(cx - b)(cy - b) = bb$.

EXEMPLUM 1

57. Sit $b=15$, $c=2$; erit $a=3^2\cdot 5\cdot 13$ et satisfieri oportet huic aequationi $(2x-15)(2y-15)=225$.

$2x-15$	1	5	9
$2y-15$	225	45	25
x	8	10	12
y	120	30	20
$x-1$	7	9*	11
$y-1$	119*	...	19
$xy-1$	...	...	239

Numeri ergo amicabiles erunt

$$\begin{cases} 3^2\cdot 5\cdot 13\cdot 11\cdot 19 \\ 3^2\cdot 5\cdot 13\cdot 239. \end{cases}$$

EXEMPLUM 2

58. Sit $b=9$, $c=2$; erit vel $a=3^2\cdot 7\cdot 13$ vel $a=3^3\cdot 5$ et aequatio resolvenda $(2x-9)(2y-9)=81$.

$2x-9$	3
$2y-9$	27
x	6
y	18
$x-1$	5
$y-1$	17
$xy-1$	107

Unde cum sit $x-1=5$, hic valor cum $a=3^3\cdot 5$ combinari nequit. Erunt ergo numeri amicabiles

$$\begin{cases} 3^2\cdot 7\cdot 13\cdot 5\cdot 17 \\ 3^2\cdot 7\cdot 13\cdot 107. \end{cases}$$

EXEMPLUM 3

59. Sit $b=21$ et $c=4$; erit $a=3^2\cdot 7^2\cdot 13$ et aequatio resolvenda $(4x-21)(4y-21)=441$.

$4x-21$	3
$4y-21$	147
x	6
y	42
$x-1$	5
$y-1$	41
$xy-1$	251

Quia x et y debent esse numeri pares, alia resolutio locum non habet.

Ex hac ergo prodeunt numeri amicabiles hi

$$\begin{cases} 3^2\cdot 7^2\cdot 13\cdot 5\cdot 41 \\ 3^2\cdot 7^2\cdot 13\cdot 251. \end{cases}$$

EXEMPLUM 4

60. Sit $b = 21$ et $c = 2$; erit $a = 3^2 \cdot 7^2 \cdot 13 \cdot 19$ et aequatio resolvenda $(2x - 21)(2y - 21) = 441$.

$2x - 21$	3	7
$2y - 21$	147	63
x	12	14
y	84	42
$x - 1$	11	13
$y - 1$	83	41
$xy - 1$	1007*	587

Quia autem valor $x - 1 = 13$ iam in valore a continetur, hinc nulli obtinentur numeri amicabiles.

EXEMPLUM 5

61. Sit $b = 57$ et $c = 2$; erit $a = 3^2 \cdot 5 \cdot 13 \cdot 19$ et aequatio resolvenda $(2x - 57)(2y - 57) = 3249$.

$2x - 57$	3	19
$2y - 57$	1083	171
x	30	38
y	570	114
$x - 1$	29	37
$y - 1$	569	113
$xy - 1$	17099	4331*

Hinc ergo oriuntur numeri amicabiles hi

$$\begin{cases} 3^2 \cdot 5 \cdot 13 \cdot 19 \cdot 29 \cdot 569 \\ 3^2 \cdot 5 \cdot 13 \cdot 19 \cdot 17099. \end{cases}$$

EXEMPLUM 6

62. Sit $b = 45$ et $c = 2$; erit $a = 3^4 \cdot 5 \cdot 11$ et aequatio resolvenda $(2x - 45)(2y - 45) = 2025$.

$2x - 45$	3	15
$2y - 45$	675	135
x	24	30
y	360	90
$x - 1$	23	29
$y - 1$	359	89
$xy - 1$	8639*	2699

Hinc ergo oriuntur numeri amicabiles

$$\begin{cases} 3^4 \cdot 5 \cdot 11 \cdot 29 \cdot 89 \\ 3^4 \cdot 5 \cdot 11 \cdot 2699. \end{cases}$$

EXEMPLUM 7

63. Sit $b = 77$ et $c = 2$; erit $a = 3^2 \cdot 7^2 \cdot 11 \cdot 13$ et aequatio resolvenda $(2x - 77)(2y - 77) = 49 \cdot 121$.

$2x - 77$	7	11
$2y - 77$	847	539
x	42	44
y	462	308
$x - 1$	41	43
$y - 1$	461	307
$xy - 1$	19403	13551*

Hinc ergo oriuntur numeri amicabiles

$$\begin{cases} 3^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 41 \cdot 461 \\ 3^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 19403. \end{cases}$$

EXEMPLUM 8

64. Sit $b = 105$, $c = 2$; erit $a = 3^2 \cdot 5 \cdot 7$ et aequatio resolvenda $2x - 105)(2y - 105) = 105^2$.

$2x - 105$	3	7	15	35
$2y - 105$	3675	...	735	...
x	54	56	60	70
y	1890	...	420	...
$x - 1$	53	55*	59	69*
$y - 1$	1889	...	419	...
$xy - 1$	102059	...	25199*	...

Cum 102059 sit numerus primus, quia continetur in forma $8a + 3$ et unico modo ad formam $2aa + bb$ reducitur, numeri amicabiles hinc orti erunt

$$\begin{cases} 3^2 \cdot 5 \cdot 7 \cdot 53 \cdot 1889 \\ 3^2 \cdot 5 \cdot 7 \cdot 102059. \end{cases}$$

SCHOLION

65. Numeri ergo amicabiles, quos hactenus ex forma apq, ar invenimus, sunt

I. $\begin{cases} 2^2 \cdot 5 \cdot 11 \\ 2^2 \cdot 71 \end{cases}$ II. $\begin{cases} 2^4 \cdot 23 \cdot 47 \\ 2^4 \cdot 1151 \end{cases}$ III. $\begin{cases} 2^7 \cdot 191 \cdot 383 \\ 2^7 \cdot 73727 \end{cases}$

IV. $\begin{cases} 4 \cdot 23 \cdot 5 \cdot 137 \\ 4 \cdot 23 \cdot 827 \end{cases}$ V. $\begin{cases} 4 \cdot 13 \cdot 17 \cdot 389 \cdot 509 \\ 4 \cdot 13 \cdot 17 \cdot 198899 \end{cases}$ VI. $\begin{cases} 3^2 \cdot 5 \cdot 13 \cdot 11 \cdot 19 \\ 3^2 \cdot 5 \cdot 13 \cdot 239 \end{cases}$

VII. $\begin{cases} 3^2\cdot 7\cdot 13\cdot 5\cdot 17 \\ 3^2\cdot 7\cdot 13\cdot 107 \end{cases}$ VIII. $\begin{cases} 3^2\cdot 7^2\cdot 13\cdot 5\cdot 41 \\ 3^2\cdot 7^2\cdot 13\cdot 251 \end{cases}$ IX. $\begin{cases} 3^2\cdot 5\cdot 13\cdot 19\cdot 29\cdot 569 \\ 3^2\cdot 5\cdot 13\cdot 19\cdot 17099 \end{cases}$

X. $\begin{cases} 3^4\cdot 5\cdot 11\cdot 29\cdot 89 \\ 3^4\cdot 5\cdot 11\cdot 2699 \end{cases}$ XI. $\begin{cases} 3^2\cdot 7^2\cdot 11\cdot 13\cdot 41\cdot 461 \\ 3^2\cdot 7^2\cdot 11\cdot 13\cdot 19403 \end{cases}$ XII. $\begin{cases} 3^2\cdot 5\cdot 7\cdot 53\cdot 1889 \\ 3^2\cdot 5\cdot 7\cdot 102059. \end{cases}$

PROBLEMA 2

66. *Invenire numeros amicabiles secundae formae* apq, ars *positis* p, q, r, s *numeris primis et factore communi* a *dato.*

SOLUTIO

Cum factor communis a detur, quaeratur ex eo valor fractionis $\frac{b}{c} = \frac{a}{2a - \int a}$ in minimis terminis hincque erit $a : \int a = b : 2b - c$. Deinde cum esse debeat $\int p \cdot \int q = \int r \cdot \int s$ seu $(p+1)(q+1) = (r+1)(s+1)$, ponatur uterque valor $= \alpha\beta xy$ et sumatur

$$p = \alpha x - 1, \quad q = \beta y - 1, \quad r = \beta x - 1, \quad s = \alpha y - 1.$$

Ubi manifestum est hos numeros α, β, x, y eiusmodi esse debere, ut p, q, r, s fiant numeri primi, et numeri amicabiles erunt

$$a(\alpha x - 1)(\beta y - 1) \quad \text{et} \quad a(\beta x - 1)(\alpha y - 1).$$

Praeterea vero ex natura numerorum amicabilium esse debet

$$\alpha\beta xy \int a = a(\alpha x - 1)(\beta y - 1) + a(\beta x - 1)(\alpha y - 1)$$

seu ob $\int a : a = 2b - c : b$ erit

$$\left.\begin{matrix} 2b\alpha\beta xy \\ -c\alpha\beta xy \end{matrix}\right\} = \begin{cases} 2b\alpha\beta xy - b\alpha x - b\beta y + 2b \\ \qquad -b\beta x - b\alpha y \end{cases}$$

vel

$$c\alpha\beta xy = b(\alpha + \beta)(x + y) - 2b.$$

Unde fit

$$\begin{aligned} cc\alpha^2\beta^2 xy &- bc\alpha\beta(\alpha+\beta)x + bb(\alpha+\beta)^2 = -2bc\alpha\beta + bb(\alpha+\beta)^2. \\ &- bc\alpha\beta(\alpha+\beta)y \end{aligned}$$

Quare satisfieri debet huic aequationi

$$(c\alpha\beta x - b(\alpha+\beta))(c\alpha\beta y - b(\alpha+\beta)) = bb(\alpha+\beta)^2 - 2bc\alpha\beta.$$

Numerus ergo $bb(\alpha+\beta)^2 - 2bc\alpha\beta$ quovis casu in duo eiusmodi factores, qui sint P, Q, resolvi debet, ut positis

$$x = \frac{P + b(\alpha+\beta)}{c\alpha\beta} \quad \text{et} \quad y = \frac{Q + b(\alpha+\beta)}{c\alpha\beta}$$

hi numeri x et y non solum fiant integri, sed etiam $\alpha x - 1$, $\beta y - 1$, $\beta x - 1$ et $\alpha y - 1$ numeri primi. Erit igitur

$$p = \frac{P + b\alpha + (b-c)\beta}{c\beta}, \quad q = \frac{Q + b\beta + (b-c)\alpha}{c\alpha},$$
$$r = \frac{P + b\beta + (b-c)\alpha}{c\alpha}, \quad s = \frac{Q + b\alpha + (b-c)\beta}{c\beta}.$$

Quovis ergo valore ipsius a proposito, unde reperitur $\frac{b}{c} = \frac{a}{2a - \int a}$, dispiciendum est, utrum cum numeri α et β ita assumi tum resolutio haec

$$bb(\alpha+\beta)^2 - 2bc\alpha\beta = PQ$$

ita institui queat, ut valores modo traditi pro p, q, r et s fiant numeri primi et tales quidem, ut factor communis a nullum eorum involvat. Quoties autem his conditionibus satisfieri poterit, erunt numeri amicabiles apq et ars.

COROLLARIUM

67. Quoniam esse nequit $\alpha = \beta$, pro his numeris α et β ponantur numeri simpliciores hincque orientur casus sequentes:

I. Sit $\alpha = 1$, $\beta = 2$; erit $PQ = 9bb - 4bc$ et

$$p = \frac{P + 3b - 2c}{2c}, \quad q = \frac{Q + 3b - c}{c},$$
$$r = \frac{P + 3b - c}{c}, \quad s = \frac{Q + 3b - 2c}{2c}.$$

II. Sit $\alpha = 1$, $\beta = 3$; erit $PQ = 16bb - 6bc$ et

$$p = \frac{P + 4b - 3c}{3c}, \quad q = \frac{Q + 4b - c}{c},$$

$$r = \frac{P + 4b - c}{c}, \quad s = \frac{Q + 4b - 3c}{3c}.$$

III. Sit $\alpha = 2$, $\beta = 3$; erit $PQ = 25bb - 12bc$ et

$$p = \frac{P + 5b}{3c} - 1, \quad q = \frac{Q + 5b}{2c} - 1,$$

$$r = \frac{P + 5b}{2c} - 1, \quad s = \frac{Q + 5b}{3c} - 1.$$

IV. Sit $\alpha = 1$, $\beta = 4$; erit $PQ = 25bb - 8bc$ et

$$p = \frac{P + 5b}{4c} - 1, \quad q = \frac{Q + 5b}{c} - 1,$$

$$r = \frac{P + 5b}{c} - 1, \quad s = \frac{Q + 5b}{4c} - 1.$$

V. Sit $\alpha = 3$, $\beta = 4$; erit $PQ = 49bb - 24bc$ et

$$p = \frac{P + 7b}{4c} - 1, \quad q = \frac{Q + 7b}{3c} - 1,$$

$$r = \frac{P + 7b}{3c} - 1, \quad s = \frac{Q + 7b}{4c} - 1.$$

VI. Sit $\alpha = 1$, $\beta = 5$; erit $PQ = 36bb - 10bc$ et

$$p = \frac{P + 6b}{5c} - 1, \quad q = \frac{Q + 6b}{c} - 1,$$

$$r = \frac{P + 6b}{c} - 1, \quad s = \frac{Q + 6b}{5c} - 1.$$

VII. Sit $\alpha = 2$, $\beta = 5$; erit $PQ = 49bb - 20bc$ et

$$p = \frac{P + 7b}{5c} - 1, \quad q = \frac{Q + 7b}{2c} - 1,$$

$$r = \frac{P + 7b}{2c} - 1, \quad s = \frac{Q + 7b}{5c} - 1.$$

VIII. Sit $\alpha = 3$, $\beta = 5$; erit $PQ = 64bb - 30bc$ et

$$p = \frac{P+8b}{5c} - 1, \quad q = \frac{Q+8b}{3c} - 1,$$
$$r = \frac{P+8b}{3c} - 1, \quad s = \frac{Q+8b}{5c} - 1.$$

IX. Sit $\alpha = 4$, $\beta = 5$; erit $PQ = 81bb - 40bc$ et

$$p = \frac{P+9b}{5c} - 1, \quad q = \frac{Q+9b}{4c} - 1,$$
$$r = \frac{P+9b}{4c} - 1, \quad s = \frac{Q+9b}{5c} - 1.$$

X. Sit $\alpha = 1$, $\beta = 6$; erit $PQ = 49bb - 12bc$ et

$$p = \frac{P+7b}{6c} - 1, \quad q = \frac{Q+7b}{c} - 1,$$
$$r = \frac{P+7b}{c} - 1, \quad s = \frac{Q+7b}{6c} - 1.$$

XI. Sit $\alpha = 5$, $\beta = 6$; erit $PQ = 121bb - 60bc$ et

$$p = \frac{P+11b}{6c} - 1, \quad q = \frac{Q+11b}{5c} - 1;$$
$$r = \frac{P+11b}{5c} - 1, \quad s = \frac{Q+11b}{6c} - 1.$$

Secundum hos igitur casus valores ipsius a iam ante adhibitos, quia prae ceteris ad numeros amicabiles inveniendos videntur apti, evolvam, ex iis autem potissimum eos eligam, qui actu ad numeros amicabiles deducunt.

EXEMPLUM 1

68. Sit $a = 2^2$; erit $b = 4$ et $c = 1$. Sumatur casus secundus, quo $\alpha = 1$, $\beta = 3$, ut numeri amicabiles sint 2^2pq et 2^2rs, fierique debet

$$PQ = 16 \cdot 16 - 6 \cdot 4 = 232$$

atque

$$p = \frac{P+16}{3} - 1, \quad q = Q + 16 - 1, \quad r = P + 16 - 1 \quad \text{et} \quad s = \frac{Q+16}{3} - 1.$$

Factores ergo numeri 232 ita debent esse comparati, ut 16 aucti fiant per 3 divisibiles.

$P = 2$	
$Q = 116$	
$P + 16 = 18$	
$Q + 16 = 132$	
$p = 5$	
$q = 131$	
$r = 17$	
$s = 43$	

Alia resolutio nulla succedit; si enim poneretur $p = 8$, fieret Q numerus impar neque ergo q et s numeri primi esse possent. Hinc ergo obtinentur hi numeri amicabiles

$$\begin{cases} 2^2 \cdot 5 \cdot 131 \\ 2^2 \cdot 17 \cdot 43. \end{cases}$$

EXEMPLUM 2

69. Si $\alpha = 1$ et $\beta = 3$ et a potestas binarii altior, inventio numerorum amicabilium non succedit, donec perveniatur ad $a = 2^8$. Tum autem erit $b = 2^8$ et $c = 1$ atque

$$PQ = 16 \cdot 2^{16} - 6 \cdot 2^8 = 2^9(2^{11} - 3) = 512 \cdot 2045 = 512 \cdot 5 \cdot 409,$$

$$p = \frac{P + 1024}{3} - 1, \quad q = Q + 1024 - 1, \quad r = P + 1024 - 1, \quad s = \frac{Q + 1024}{3} - 1,$$

unde factores P et Q ita debent esse comparati, ut quaternario aucti per 3 vel, ut quoti fiant pares, per 6 sint divisibiles.

$P =$	2	8	20	32	80	128	320	1280
$Q =$	. . .	. . .	. . .	. . .	13088	8180	. . .	. . .
$P + 1024 =$	1026	1032	1044	1056	1104	1152	1344	2304
$Q + 1024 =$	. . .	. . .	. . .	. . .	14112	9204	. . .	. . .
$p =$	341*	343*	347	. . .	367	383	447*	767*
$q =$	. . .	. . .	. . .	. . .	14111*	9203	. . .	. . .
$r =$	1025*	. . .	1043*	1055*	1103	1151	1343*	2303*
$s =$	. . .	. . .	. . .	. . .	4703	3067	. . .	. . .

Erunt ergo numeri amicabiles $\begin{cases} 2^8 \cdot 383 \cdot 9203 \\ 2^8 \cdot 1151 \cdot 3067. \end{cases}$

EXEMPLUM 3

70. Sit $\alpha = 2$ et $\beta = 3$ et sumatur $a = 3^2 \cdot 5 \cdot 13$, ut sit $b = 15$ et $c = 2$; erit

$$PQ = 25 \cdot 225 - 12 \cdot 30 = 3^4 \cdot 5 \cdot 13,$$

$$p = \frac{P+75}{6} - 1, \quad q = \frac{Q+75}{4} - 1, \quad r = \frac{P+75}{4} - 1, \quad s = \frac{Q+75}{6} - 1,$$

unde factores PQ eiusmodi esse debent, ut ternario aucti fiant per 24 divisibiles.

$P = 45$	
$Q = 117$	
$P + 75 = 120$	
$Q + 75 = 192$	
$p = 19$	
$q = 47$	
$r = 29$	
$s = 31$	

Aliae resolutiones non inveniunt locum; unde hinc numeri amicabiles prodeunt

$$\begin{cases} 3^2 \cdot 5 \cdot 13 \cdot 19 \cdot 47 \\ 3^2 \cdot 5 \cdot 13 \cdot 29 \cdot 31. \end{cases}$$

EXEMPLUM 4

71. Sit $\alpha = 1$ et $\beta = 4$ et sumatur $a = 3^3 \cdot 5$, ut sit $b = 9$ et $c = 2$; erit

$$PQ = 25 \cdot 81 - 8 \cdot 18 = 9 \cdot 11 \cdot 19$$

et

$$p = \frac{P+45}{8} - 1, \quad q = \frac{Q+45}{2} - 1, \quad r = \frac{P+45}{2} - 1, \quad s = \frac{Q+45}{8} - 1,$$

unde P et Q eiusmodi debent esse numeri, ut quinario aucti per 8 fiant divisibiles.

$P =$	3	19
$Q =$	627	99
$P + 45 =$	48	64
$Q + 45 =$	672	144
$p =$	5	7
$q =$	335*	71
$r =$	23	31
$s =$	83	17

Hinc ergo oriuntur numeri amicabiles

$$\begin{cases} 3^3 \cdot 5 \cdot 7 \cdot 71 \\ 3^3 \cdot 5 \cdot 31 \cdot 17. \end{cases}$$

SCHOLION

72. Hae autem operationes nimis sunt incertae ac plerumque plures frustra instituuntur, antequam numeri amicabiles se offerunt. Labor quoque foret vehementer prolixus, si singulis valoribus ipsius a, quos quidem supra exhibui, per singulos casus litterarum α et β percurrere velimus; atque nimis raro evenit, ut quatuor numeri pro p, q, r et s resultantes simul fiant primi. Tum vero etiam inventio numerorum amicabilium per determinationem rationis α et β nimis restringitur atque dantur casus huiusmodi numerorum, in quibus ratio $\alpha:\beta$ tam est complicata, ut nulla probabili ratione eligi potuisset; cuiusmodi sunt numeri amicabiles $2^4 \cdot 19 \cdot 8563$ et $2^4 \cdot 83 \cdot 2039$[1], ad quos hac via inveniendos ratio $\alpha:\beta$ assumi debuisset $5:21$ vel $1:102$. Hanc ob rem huic methodo nimis sterili et operosae diutius non immoror, sed aliam viam aperiam, qua facilius et expeditius numeros amicabiles tam huius secundae formae quam aliarum magis compositarum investigare liceat et quae similis sit praecedenti, quae tribus tantum numeris primis reperiendis absolvitur.

PROBLEMA 3

73. *Invenire numeros amicabiles huius formae apq et afr, ubi p, q et r sint numeri primi, f sive primus sive compositus, qui perinde ac factor communis a sit datus.*

SOLUTIO

Quaerantur iterum ex cognito factore communi a valores b et c, ut sit $\frac{b}{c} = \frac{a}{2a - \int a}$, et sit numeri f summa divisorum $\int f = gh$. Cum igitur primo requiratur, ut sit $\int p \cdot \int q = \int f \cdot \int r$, erit $(p+1)(q+1) = gh(r+1)$. Ponatur $r + 1 = xy$, $p + 1 = hx$ et $q + 1 = gy$ et necesse erit, ut sint hi tres numeri primi, scilicet $p = hx - 1$, $q = gy - 1$ et $r = xy - 1$. Deinde opus est, ut sit

$$\int apq = ghxy \int a = a(hx-1)(gy-1) + af(xy-1)$$
$$= a((gh+f)xy - hx - gy + 1 - f)$$

1) Sed vide notam p. 61. F. R.

seu

$$2bghxy - cghxy = b(gh+f)xy - bhx - bgy + b(1-f)$$

vel

$$(bf - bgh + cgh)xy - bhx - bgy = b(f-1).$$

Ponamus brevitatis gratia

$$bf - bgh + cgh = e;$$

erit $eexy - ebhx - ebgy = eb(f-1)$ sive

$$(ex - bg)(ey - bh) = bbgh + be(f-1).$$

Numerus ergo $bbgh + be(f-1)$ in duos eiusmodi factores, qui sint P et Q, resolvi debet, ut fiant

$$x = \frac{P+bg}{e} \quad \text{et} \quad y = \frac{Q+bh}{e}$$

numeri integri, tum vero $hx-1$, $gy-1$ et $xy-1$ numeri primi. Quae conditio quoties impleri poterit, erunt numeri amicabiles $a(hx-1)(gy-1)$ et $af(xy-1)$. Notandum est neque ullum horum numerorum primorum $hx-1$, $gy-1$, $xy-1$ neque ullum factorem ipsius f divisorem esse debere ipsius a nec non f et $xy-1$ esse debere numeros primos inter se.

COROLLARIUM 1

74. Si f sit numerus primus, uti secunda forma numerorum amicabilium postulat, erit $f+1 = gh$ et propterea $f = gh - 1$. Hoc ergo casu erit $e = cgh - b$ et $PQ = bbgh + be(gh-2)$ seu

$$PQ = bcgghh - 2bcgh + 2bb.$$

Unde quaeri debent numeri x et y supra memoratis proprietatibus praediti, ut sit

$$x = \frac{P+bg}{e} \quad \text{et} \quad y = \frac{Q+bh}{e}.$$

COROLLARIUM 2

75. His igitur formulis ita uti conveniet, ut pro a successive alii atque alii valores ex iis, quos supra exposui, substituantur atque pro singulis litterae f varii numeri tam primi quam compositi substituantur, qui quidem ad numeros amicabiles inveniendos idonei videantur.

CASUS 1

76. Sit $a=4$ (ex valore enim $a=2$ nullos obtineri numeros amicabiles observavi) eritque $b=4$ et $c=1$. Tum positis numeris amicabilibus $4pq$ et $4fr$ sit $\int f=gh$ et $e=4f-3gh$. Deinde per resolutionem quaerantur factores P et Q, ut sit

$$PQ=16gh+4e(f-1).$$

Hincque eruantur numeri integri x et y, ut sit

$$x=\frac{P+4g}{e} \quad \text{et} \quad y=\frac{Q+4h}{e},$$

et ex his deriventur valores litterarum $p=hx-1$, $q=gy-1$ et $r=xy-1$; qui si fuerint numeri primi, erunt $4pq$ et $4fr$ numeri amicabiles.

EXEMPLUM 1

77. Sit $f=3$; erit $\int f=gh=4$ hincque $e=12-12=0$, unde patet ex hac hypothesi nihil obtineri.

EXEMPLUM 2

78. Sit $f=5$; erit $\int f=gh=6$, $e=20-18=2$ atque

$$PQ=16\cdot 6+8\cdot 4=128.$$

Iam ex $gh=6$ ponatur primo $g=2$ et $h=3$ fietque

$$x=\frac{P+8}{2} \quad \text{et} \quad y=\frac{Q+12}{2}.$$

Quare sequentes habebuntur resolutiones:

$P=$	2	4	8	16	32	64
$Q=$	64	32	16	8	4	2
$x=$	5	6	8	12	20	2
$y=$	38	22	14	10	8	36
$p=3x-1=$	14*	17	23	35*	59	7
$q=2y-1=$	...	43	27*	19	15*	107
$r=xy-1=$	...	131	111*	119*	159*	251

Hinc ergo prodeunt numeri amicabiles

$$\begin{cases}4\cdot 17\cdot 43\\ 4\cdot 5\cdot 131\end{cases} \quad \text{et} \quad \begin{cases}4\cdot 13\cdot 107\\ 4\cdot 5\cdot 251.\end{cases}$$

Ponatur secundo $g=1$, $h=6$ fietque

$$x=\frac{P+4}{2} \quad \text{et} \quad y=\frac{Q+24}{2}.$$

$P=$	2	4	8	16	32	64
$Q=$	64	32	16	8	4	2
$x=$	3	4	6	10	18	34
$y=$	44	28	20	16	14	13
$p=6x-1=$	17	23	35*	59	107	203*
$q=1y-1=$	43	27*	19	15*	13	12*
$r=xy-1=$	131	111*	119*	159*	251	441*

Iidem ergo prodeunt bini numeri amicabiles qui ante.

Sunt ergo hinc numeri amicabiles

$$\begin{cases} 4\cdot 17\cdot 43 \\ 4\cdot 5\cdot 131 \end{cases} \quad \text{et} \quad \begin{cases} 4\cdot 13\cdot 107 \\ 4\cdot 5\cdot 251. \end{cases}$$

EXEMPLUM 3

79. Sit $f=7$; erit $\int f=gh=8$, $e=28-24=4$ et

$$PQ=16\cdot 8+16\cdot 6=224.$$

Sit ergo primo $g=2$, $h=4$; erit

$$x=\frac{P+8}{4}, \quad y=\frac{Q+16}{4}, \quad p=4x-1, \quad q=2y-1, \quad r=xy-1.$$

P	4	8	28	56
Q	56	28	8	4
x	3	4	9	16
y	18	11	6	5
$4x-1$	11	15*	35*	63*
$2y-1$	35*	21*	11	9*
$xy-1$	53	43	53	79

Sit secundo $g=1$, $h=8$; erit

$$x=\frac{P+4}{4},\quad y=\frac{Q+32}{4},\quad p=8x-1,\quad q=y-1,\quad r=xy-1.$$

P	4	8	28	56
Q	56	28	8	4
x	2	3	8	15
y	22	15	10	9
$8x-1$	15*	23	63*	119*
$y-1$	21*	14*	9*	8*
$xy-1$	43	44*	79	134*

Hinc ergo nulli prodeunt numeri amicabiles.

EXEMPLUM 4

80. Sit $f=11$; erit $gh=12$, $e=8$, $PQ=16\cdot 12+32\cdot 10=512$, vel erit $(8x-4g)(8y-4h)=512$, quae aequatio deprimitur ad $(2x-g)(2y-h)=32$; qua resoluta erit $p=hx-1$, $q=gy-1$ et $r=xy-1$. Sive autem hic ponatur $g=1$, $h=12$, sive $g=2$, $h=6$, sive $g=3$, $h=4$, nulli prodeunt numeri primi pro p, q et r.

EXEMPLUM 5

81. Sit $f=13$; erit $gh=14$, $e=10$, $PQ=224+40\cdot 12=704$ et $(10x-4g)(10y-4h)=704$, quae deprimitur ad $(5x-2g)(5y-2h)=176$. Hinc autem nulli alii numeri amicabiles obtinentur nisi

$$\begin{cases} 4\cdot 5\cdot 251 \\ 4\cdot 13\cdot 107, \end{cases}$$

qui iam ante (§ 78) sunt inventi. Simul vero iam patet, etiamsi pro f maiores numeri primi statuantur, nullos novos numeros amicabiles prodire, quoniam vel p vel q sortietur valorem minorem, qui pro f assumi potuisset.

EXEMPLUM 6

82. Sit $f=5\cdot 13$; erit $gh=6\cdot 14=84$, $e=8$, $PQ=16\cdot 84+32\cdot 64=64\cdot 53$ et $(8x-4g)(8y-4h)=64\cdot 53$ seu $(2x-g)(2y-h)=4\cdot 53$. Hincque in-

venietur in numeris primis $p = 43$, $q = 2267$ et $r = 1187$, unde erunt numeri amicabiles

$$\begin{cases} 4 \cdot 43 \cdot 2267 \\ 4 \cdot 5 \cdot 13 \cdot 1187. \end{cases}$$

CASUS 2

83. Sit $a = 2^3 = 8$; erit $b = 8$, $c = 1$; tum positis numeris amicabilibus $8pq$ et $8fr$ et $\int f = gh$ erit $e = 8f - 7gh$ atque

$$(ex - 8g)(ey - 8h) = 64gh + 8e(f - 1),$$

unde casus sunt dignoscendi, quibus fiunt numeri primi

$$p = hx - 1, \quad q = gy - 1 \quad \text{et} \quad r = xy - 1.$$

EXEMPLUM 1

84. Sit $f = 11$; erit $gh = 12$, $e = 4$ atque

$$(4x - 8g)(4y - 8h) = 64 \cdot 12 + 32 \cdot 10 = 64 \cdot 17$$

seu

$$(x - 2g)(y - 2h) = 4 \cdot 17 = 68.$$

Hinc autem nulli numeri amicabiles reperiuntur.

EXEMPLUM 2

85. Sit $f = 13$; erit $gh = 14$, $e = 6$ atque

$$(6x - 8g)(6y - 8h) = 64 \cdot 14 + 48 \cdot 12 = 64 \cdot 23$$

seu

$$(3x - 4g)(3y - 4h) = 16 \cdot 23;$$

verum etiam haec hypothesis est inutilis.

EXEMPLUM 3

86. Sit $f = 17$; erit $gh = 18$, $e = 10$ atque

$$(10x - 8g)(10y - 8h) = 64 \cdot 18 + 80 \cdot 16 = 64 \cdot 38$$

seu

$$(5x - 4g)(5y - 4h) = 32 \cdot 19;$$

hincque prodeunt numeri amicabiles

$$\begin{cases} 8 \cdot 23 \cdot 59 \\ 8 \cdot 17 \cdot 79. \end{cases}$$

EXEMPLUM 4

87. Magis foecunda est hypothesis $f = 11 \cdot 23$; minor enim valor pro f in compositis substitui nequit; erit $gh = 12 \cdot 24$, $e = 8$, unde

$$(8x - 8g)(8y - 8h) = 64 \cdot 12 \cdot 24 + 64 \cdot 252$$

seu

$$(x - g)(y - h) = 540.$$

Hinc autem reperiuntur sequentes numeri amicabiles

$$\begin{cases} 8 \cdot 383 \cdot 1907 \\ 8 \cdot 11 \cdot 23 \cdot 2543 \end{cases} \quad \begin{cases} 8 \cdot 467 \cdot 1151 \\ 8 \cdot 11 \cdot 23 \cdot 1871 \end{cases} \quad \begin{cases} 8 \cdot 647 \cdot 719 \\ 8 \cdot 11 \cdot 23 \cdot 1619. \end{cases}$$

Huiusmodi numeris compositis pro f ponendis multi insuper alii inveniuntur numeri amicabiles.

SCHOLION

88. Ingens combinationum numerus, qui in hoc exemplo locum habet, ansam mihi praebuit solutionem in aliam formam redigendi commodiorem. Scilicet cum sit

$$e = bf - (b - c)gh, \quad PQ = bbgh + be(f - 1) = (ex - bg)(ey - bh),$$

ex formulis

$$x = \frac{P + bg}{e} \quad \text{et} \quad y = \frac{Q + bh}{e}$$

eliciuntur valores

$$p = \frac{hP + bgh}{e} - 1, \quad q = \frac{gQ + bgh}{e} - 1, \quad r = \frac{PQ + b(hP + gQ) + bbgh}{ee} - 1.$$

Sit ergo ob $gh = \int f$

erit

$$e = bf - (b - c)\int f, \quad L = bb\int f + be(f - 1) \quad \text{et} \quad MN = L\int f;$$

$$p = \frac{M + b\int f}{e} - 1, \quad q = \frac{N + b\int f}{e} - 1, \quad r = \frac{L + b(M + N) + bb\int f}{ee} - 1$$

et nunc quaestio eo reducitur, ut numerus $L\int f$ resolvatur in duos factores M et N, quorum uterque quantitate $b\int f$ auctus fiat divisibilis per e et ut quoti hinc resultantes unitate minuti sint numeri primi. Denique oportet, ut sit $r + 1 = \frac{(p+1)(q+1)}{\int f}$ et r numerus primus. Hunc ergo calculum in nonnullis casibus illustrabo.

CASUS 3

89. Sit $a = 2^4 = 16$; erit $b = 16$, $c = 1$ atque

$$e = 16f - 15\int f, \quad L = 256\int f + 16e(f - 1) \quad \text{et} \quad MN = L\int f.$$

Numeri igitur primi esse debent

$$p = \frac{M + 16\int f}{e} - 1, \quad q = \frac{N + 16\int f}{e} - 1, \quad r = \frac{L + 256\int f + 16(M + N)}{ee} - 1,$$

quibus inventis erunt numeri amicabiles $16pq$ et $16fr$.

EXEMPLUM 1

90. Sit $f = 17$; erit

$$\int f = 18, \quad e = 2, \quad L = 1024 \cdot 5 \quad \text{et} \quad MN = 1024 \cdot 5 \cdot 18 = 2^{11} \cdot 3^2 \cdot 5,$$

$$p = \frac{M + 288}{2} - 1, \quad q = \frac{N + 288}{2} - 1, \quad r = \frac{512 \cdot 19 + 16(M + N)}{4} - 1;$$

seu sit $M = 2m$, $N = 2n$, ut sit $mn = 2^9 \cdot 3^2 \cdot 5$; erit

$$p = m + 143, \quad q = n + 143 \quad \text{et} \quad r = 8(m + n) + 2431,$$

qui tres numeri debent esse primi, ut numeri amicabiles sint $16pq$ et $16\cdot 17r$. Hoc autem succedit duobus modis, primo, si $m=24$, $n=960$, et secundo, si $m=96$ et $n=240$; unde numeri amicabiles prodeunt

$$\begin{cases}16\cdot 167\cdot 1103\\ 16\cdot 17\cdot 10303\end{cases}\qquad \begin{cases}16\cdot 239\cdot 383\\ 16\cdot 17\cdot 5119.\end{cases}$$

EXEMPLUM 2

91. Sit $f=19$; erit

$$\int f=20,\quad e=4,\quad L=128\cdot 49\quad \text{et}\quad MN=512\cdot 5\cdot 49=2^9\cdot 5\cdot 7^2.$$

Ergo

$$p=\frac{M+320}{4}-1,\quad q=\frac{N+320}{4}-1,\quad r=\frac{128\cdot 89+16(M+N)}{16}-1;$$

seu sit $M=4m$ et $N=4n$, ut sit $mn=32\cdot 5\cdot 49=2^5\cdot 5\cdot 7^2$; erit

$$p=m+79,\quad q=n+79\quad \text{et}\quad r=4(m+n)+711.$$

Hinc, si $m=70$, $n=112$, prodeunt numeri amicabiles

$$\begin{cases}16\cdot 149\cdot 191\\ 16\cdot 19\cdot 1439.\end{cases}$$

EXEMPLUM 3

92. Sit $f=23$; erit

$$\int f=24,\quad e=8,\quad L=256\cdot 5\cdot 7\quad \text{et}\quad MN=2048\cdot 3\cdot 5\cdot 7=2^{11}\cdot 3\cdot 5\cdot 7,$$

$$p=\frac{M+16\cdot 24}{8}-1,\quad q=\frac{N+16\cdot 24}{8}-1,\quad r=\frac{256\cdot 59+16(M+N)}{64}-1;$$

seu sit $M=8m$, $N=8n$ et $mn=2^5\cdot 3\cdot 5\cdot 7$; erit

$$p=m+47,\quad q=n+47\quad \text{et}\quad r=2(m+n)+235.$$

Hinc tres casus oriuntur

$$\begin{cases}m=56\\ n=60\end{cases}\qquad \begin{cases}m=42\\ n=80\end{cases}\qquad \begin{cases}m=6\\ n=560\end{cases}$$

et numeri amicabiles sunt

$$\begin{cases}16\cdot 103\cdot 107\\ 16\cdot 23\cdot 467\end{cases}\qquad \begin{cases}16\cdot 89\cdot 127\\ 16\cdot 23\cdot 479\end{cases}\qquad \begin{cases}16\cdot 53\cdot 607\\ 16\cdot 23\cdot 1367.\end{cases}$$

EXEMPLUM 4

93. Sit $f=31$; erit

$$\int f=32,\quad [e=16],\quad L=512\cdot 31\quad \text{et}\quad MN=2^{14}\cdot 31,$$

$$p=\frac{M+16\cdot 32}{16}-1,\quad q=\frac{N+16\cdot 32}{16}-1,\quad r=\frac{16(M+N)+512\cdot 47}{256}-1.$$

Sit ergo $M=16m$, $N=16n$, ut sit $mn=2^6\cdot 31$; erit

$$p=m+31,\quad q=n+31,\quad r=m+n+93.$$

Hinc autem nulli prodeunt numeri amicabiles.

EXEMPLUM 5

94. Sit $f=47$; erit

$$\int f=48,\quad e=32\quad \text{et}\quad L=1024\cdot 5\cdot 7\quad \text{et}\quad MN=2^{14}\cdot 3\cdot 5\cdot 7,$$

unde

$$p=\frac{M+16\cdot 48}{32}-1,\quad q=\frac{N+16\cdot 48}{32}-1\quad \text{et}\quad r=\frac{16(M+N)+1024\cdot 47}{1024}-1.$$

Sit $M=32m$ et $N=32n$, ut sit $mn=2^4\cdot 3\cdot 5\cdot 7$; erit

$$p=m+23,\quad q=n+23,\quad r=\tfrac{1}{2}(m+n)+46.$$

Ergo $m+n$ debet esse numerus impariter par, ut $\frac{1}{2}(m+n)$ fiat impar, quod evenit, si vel m vel n sit impariter par. Sit $m=30$, $n=56$; erunt numeri amicabiles

$$\begin{cases}16\cdot 53\cdot 79\\ 16\cdot 47\cdot 89.\end{cases}$$

EXEMPLUM 6

94[a][1]). Sit $f = 17 \cdot 137$; erit

$$\int f = 18 \cdot 138 = 4 \cdot 27 \cdot 23 = 2484, \quad e = 4,$$

$$L = 256 \cdot 2484 + 64 \cdot 2328 = 512 \cdot 3 \cdot 7 \cdot 73 \quad \text{et} \quad MN = 2048 \cdot 81 \cdot 7 \cdot 23 \cdot 73,$$

$$p = \frac{M + 16 \cdot 2484}{4} - 1, \quad q = \frac{N + 16 \cdot 2484}{4} - 1, \quad r = \frac{512 \cdot 2775 + 16(M+N)}{16} - 1.$$

Sit $M = 4m$, $N = 4n$; erit $mn = 128 \cdot 81 \cdot 7 \cdot 23 \cdot 73$ et

$$p = m + 9935, \quad q = n + 9935 \quad \text{et} \quad r = 4(m+n) + 88799.$$

Sed hic semper prodit valor ipsius r maior quam 100000, ita ut difficile sit discernere, utrum sit primus necne.

EXEMPLUM 7

95. Sit $f = 17 \cdot 151$; erit

$$\int f = 18 \cdot 152 = 16 \cdot 9 \cdot 19 = 276, \quad e = 32,$$

$$L = 1024 \cdot 1967 = 1024 \cdot 7 \cdot 281 \quad \text{atque} \quad MN = 2^{14} \cdot 9 \cdot 7 \cdot 19 \cdot 281.$$

Sit $M = 32m$, $N = 32n$; erit $mn = 16 \cdot 9 \cdot 7 \cdot 19 \cdot 281$ et

$$p = m + 1367, \quad q = n + 1367, \quad r = \tfrac{1}{2}(m+n) + 2650.$$

Sit $m = 2\mu$, $n = 8\nu$; erit $\mu\nu = 9 \cdot 7 \cdot 19 \cdot 281$ et

$$p = 2\mu + 1367, \quad q = 8\nu + 1367, \quad r = \mu + 4\nu + 2650.$$

Hinc primum patet neque μ neque ν esse posse numerum formae $3\alpha + 2$, tum μ non posse desinere in 9 nec ν in 1; quibus observatis sequentes tantum resolutiones locum habent:

	*				*	*	
μ	$3 \cdot 281$	$7 \cdot 19$	$21 \cdot 281$	21	$63 \cdot 281$	3	1
ν	$21 \cdot 19$	$9 \cdot 281$	57	$57 \cdot 281$	19	$399 \cdot 281$	$1197 \cdot 281$

1) In editione principe falso numerus 94 iteratur. F. R.

quorum ii, qui asteriscis sunt notati, excluduntur ideo, ne p, q vel r fiat per 7 divisibile. Quarta resolutio dabit hos numeros amicabiles

$$\begin{cases} 16 \cdot 1409 \cdot 129503 \\ 16 \cdot 17 \cdot 151 \cdot 66739, \end{cases}$$

si modo hic numerus 129503 est primus.[1])

EXEMPLUM 8

96. Sit $f = 17 \cdot 167$; erit

$$\int f = 18 \cdot 168 = 16 \cdot 27 \cdot 7 = 3024, \quad e = 64,$$

$$L = 2048 \cdot 1797 = 2048 \cdot 3 \cdot 599 \quad \text{et} \quad MN = 2^{15} \cdot 3^4 \cdot 7 \cdot 599.$$

Sit $M = 64m$, $N = 64n$; erit $mn = 2^3 \cdot 3^4 \cdot 7 \cdot 599$ et

$$p = m + 755, \quad q = n + 755, \quad r = \tfrac{1}{4}(m+n) + \tfrac{2173}{2}.$$

Sit $m = 2\mu$, $n = 4\nu$; erit $\mu\nu = 3^4 \cdot 7 \cdot 599$ et

$$p = 2\mu + 755, \quad q = 4\nu + 755, \quad r = \nu + \frac{\mu+1}{2} + 1086.$$

Ubi patet esse oportere $\mu = 4\alpha - 1$, ne r fiat numerus par, nec $\mu = 3\alpha + 2$ nec $\nu = 3\alpha + 1$. Hinc prodeunt numeri amicabiles

$$\begin{cases} 16 \cdot 809 \cdot 51071 \\ 16 \cdot 17 \cdot 167 \cdot 13679. \end{cases}$$

CASUS 4

97. Sit vel $a = 3^3 \cdot 5$ vel $a = 3^2 \cdot 7 \cdot 13$, ut sit $b = 9$, $c = 2$; erit

$$e = 9f - 7\int f, \quad L = 81\int f + 9e(f-1) \quad \text{et} \quad MM = L\int f,$$

$$p = \frac{M + 9\int f}{e} - 1, \quad q = \frac{N + 9\int f}{e} - 1, \quad r = \frac{9(M+N) + L + 81\int f}{ee} - 1;$$

qui numeri p, q, r si fuerint primi, erunt numeri amicabiles apq et afr.

1) Est autem $129503 = 11 \cdot 61 \cdot 193$ ideoque numeri correspondentes non sunt amicabiles. F. R.

EXEMPLUM

98. Sit $f=7$, $\int f=8$; erit

$$e=7, \quad L=2\cdot 27\cdot 19, \quad MN=16\cdot 27\cdot 19,$$

$$p=\frac{M+72}{7}-1, \quad q=\frac{N+72}{7}-1, \quad r=\frac{9(M+N)+2\cdot 27\cdot 31}{49}-1.$$

Unde posito $M=54$, $N=152$ oriuntur numeri amicabiles

$$\begin{cases} a\cdot 17\cdot 31 \\ a\cdot 7\cdot 71 \end{cases} \quad \text{seu} \quad \begin{cases} 3^3\cdot 5\cdot 17\cdot 31 \\ 3^3\cdot 5\cdot 7\cdot 71. \end{cases}$$

PROBLEMA 4

99. *Invenire numeros amicabiles huius formae* $agpq$ *et* ahr, *ubi* p, q, r *sint numeri primi, at* g *et* h *sive primi sive compositi dati una cum factore communi* a.

SOLUTIO

Ex factore communi a quaeratur in minimis terminis fractio $\frac{b}{c}=\frac{a}{2a-\int a}$, deinde sit $\frac{\int g}{\int h}=\frac{m}{n}$ et ex prima proprietate numerorum amicabilium erit

$$(p+1)(q+1)\int g=(r+1)\int h \quad \text{seu} \quad r+1=\frac{m}{n}(p+1)(q+1).$$

Altera vero proprietas praebet

$$(r+1)\int a\cdot\int h=a(gpq+hr);$$

vel ob $\frac{\int a}{a}=\frac{2b-c}{b}$ erit

$$(r+1)(2b-c)\int h=b(gpq+hr)$$

et pro r substituto valore

$$m(2b-c)(p+1)(q+1)\int h=b(ngpq+mh(p+1)(q+1)-nh).$$

Sit brevitatis gratia $p+1=x$, $q+1=y$; erit

$$m(2b-c)xy\int h = b(mhxy+ngxy-ngx-ngy+ng-nh)$$

vel

$$\left(mbh+nbg-2mb\int h+mc\int h\right)xy-nbgx-nbgy=nb(h-g).$$

Ponatur brevitatis gratia

$$e=b(mh+ng)-(2b-c)m\int h$$

eritque

$$eexy-nbgex-nbgey+nnbbgg=nnbbgg+nb(h-g)e$$

seu

$$(ex-nbg)(ey-nbg)=nnbbgg+nb(h-g)e.$$

Ponatur ergo $nnbbgg+nb(h-g)e=MN$ fietque

$$x=\frac{M+nbg}{e} \quad \text{et} \quad y=\frac{N+nbg}{e}$$

seu

$$p=\frac{M+nbg}{e}-1,\quad q=\frac{N+nbg}{e}-1,\quad r=\frac{m}{n}xy-1.$$

Qui tres numeri p, q et r si fuerint primi, erunt numeri amicabiles $agpq$ et ahr, dummodo utriusque factores sint primi inter se.

COROLLARIUM

100. Si sint g et h numeri primi, erit $\frac{m}{n}=\frac{g+1}{h+1}$; sit ergo $g=km-1$ et $h=kn-1$; erit $\int h=kn$, unde fiet

$$e=b(2kmn-m-n)-(2b-c)kmn=ckmn-b(m+n),$$

$$MN=nb\left(nb(km-1)^2+k(n-m)e\right)=\left(ex-bn(km-1)\right)\left(ey-bn(km-1)\right)$$

et

$$p=x-1,\quad q=y-1\quad \text{atque}\quad r=\frac{m}{n}xy-1.$$

CASUS 1

101. Sit $m=1$, $n=3$, ergo $g=k-1$, $h=3k-1$ eritque

$$e=3ck-4b \quad \text{et} \quad MN=3b(3b(k-1)^2+2ke)$$

ideoque

$$x=\frac{M+3b(k-1)}{e}, \quad y=\frac{N+3b(k-1)}{e}$$

ac denique $p=x-1$, $q=y-1$ et $r=\frac{1}{3}xy-1$.

EXEMPLUM 1

102. Sit $a=4$, $b=4$, $c=1$; erit

$$e=3k-16 \quad \text{et} \quad MN=12(12(k-1)^2+2ke)$$

et

$$x=\frac{M+12(k-1)}{e} \quad \text{et} \quad y=\frac{N+12(k-1)}{e}.$$

Hic poni potest

I. $k=6$ fietque $g=5$, $h=17$ et $e=2$, sed hinc nihil efficitur.

II. $k=8$ fietque $g=7$, $h=23$ et $e=8$, $MN=12(12\cdot 49+128)$ seu $MN=16\cdot 3\cdot 179=(8x-84)(8y-84)$ ideoque $3\cdot 179=(2x-21)(2y-21)$, unde nihil pariter sequitur.

EXEMPLUM 2

103. Sit $a=8$, $b=8$, $c=1$; erit

$$e=3k-32, \quad MN=24(24(k-1)^2+2ke)$$

seu

$$MN=48\big(15kk-56k+12\big)=\big(ex-24(k-1)\big)\big(ey-24(k-1)\big).$$

Verum ne hinc quoque quicquam concludere licet.

CASUS 2

104. Sit $m=3$, $n=1$; erit

$$e=3ck-4b \quad \text{et} \quad g=3k-1, \quad h=k-1,$$

$$MN=b\big(b(3k-1)^2-2ke\big)=\big(ex-b(3k-1)\big)\big(ey-b(3k-1)\big)$$

atque $p=x-1$, $q=y-1$ et $r=3xy-1$.

EXEMPLUM 1

105. Sit $a=10$, $b=5$, $c=1$; erit

$$e=3k-20 \quad \text{et} \quad 5\big(5(3k-1)^2-2ke\big)=\big(ex-5(3k-1)\big)\big(ey-5(3k-1)\big).$$

Si hic ponatur $k=8$, fiet $5\cdot 29\cdot 89=(4x-115)(4y-115)$. Unde prodit $x=30$, $y=674$, $3xy=60660$ et numeri amicabiles erunt

$$\begin{cases} 10\cdot 23\cdot 29\cdot 673 \\ 10\cdot 7\cdot 60659. \end{cases}$$

EXEMPLUM 2

106. Sit $a=3^3\cdot 5$, $b=9$, $c=2$; erit

$$e=6k-36 \quad \text{et} \quad 9(3k-1)^2-2ke=\Big(\frac{1}{3}\,ex-3(3k-1)\Big)\Big(\frac{1}{3}\,ey-3(3k-1)\Big).$$

Iam fiat $k=8$; erit $e=12$ et $3\cdot 1523=(4x-69)(4y-69)$ hincque oritur $x=18$, $y=398$, $3xy=21492$ eruntque numeri primi $g=23$, $h=7$, $p=17$, $q=397$, $r=21491$ et numeri amicabiles

$$\begin{cases} 3^3\cdot 5\cdot 23\cdot 17\cdot 397 \\ 3^3\cdot 5\cdot 7\cdot 21491. \end{cases}$$

SCHOLION

107. Ex his exemplis usus huius problematis in inveniendis numeris amicabilibus satis luculenter perspicitur; sed ob ipsam nimiam fingendi libertatem non parum molestum est secundum praecepta hic tradita omnes casus percurrere. Cum igitur sufficiat hanc methodum tradidisse eiusque usum monstrasse, ei prolixius non immoror, sed ad ultimam methodum, cuius ope numeros amicabiles eruere liceat, qua quidem sum usus, exponendam progredior. Nititur ea autem singularibus proprietatibus, quibus numeri ratione summae divisorum gaudent, quas oblata occasione explicabo[1]), ne plurium lemmatum praemissio taedium creet. Iis autem expositis non difficile erit plura alia problemata ad hoc genus pertinentia resolvere.

1) Vide ex. gr. Commentationem 243 huius voluminis. F. R.

PROBLEMA 5

108. *Invenire numeros amicabiles huius formae zap et zbq, ubi factores a et b sint dati, p et q numeri primi et factor communis z investigari debeat.*

SOLUTIO

Sit $\int a : \int b = m : n$, et cum esse debeat $\int a \cdot (p+1) = \int b \cdot (q+1)$, erit $m(p+1) = n(q+1)$. Ponatur $p+1 = nx$ et $q+1 = mx$ eruntque numeri amicabiles

$$za(nx-1) \quad \text{et} \quad zb(mx-1),$$

ubi quidem requiritur, ut $mx-1$ et $nx-1$ sint numeri primi. Cum iam utriusque numeri eadem sit summa divisorum $= nx\int a \cdot \int z = mx \int b \cdot \int z$, oportet, ut ea sit aequalis summae numerorum $z((na+mb)x-a-b)$. Unde obtinetur ista aequatio

$$\frac{z}{\int z} = \frac{nx\int a}{(na+mb)x-a-b}.$$

Quo iam ex hac aequatione valor ipsius z elici queat, fractio $\frac{nx\int a}{(na+mb)x-a-b}$ ad minimos terminos reducatur, quae sit $= \frac{r}{s}$, ita ut habeatur $\frac{z}{\int z} = \frac{r}{s}$, hincque sequentia sunt notanda. Primo esse z vel ipsi r aequale vel eius multiplo cuipiam, puta kr. Priori casu, si $z = r$, erit $\int z = s$ ac propterea $s = \int r$. Posteriori casu, si $z = kr$, erit $\int z = ks = \int kr$. Verum quicquid sit k, erit $\frac{\int kr}{\int r} > k$; nam $\int kr$ continet omnes divisores ipsius r singulos per k multiplicatos et insuper eos divisores ipsius kr[1]), qui non sunt per k divisibiles, eritque ergo $\int kr > k\int r$. Cum igitur sit $\int z > k\int r$, erit quoque $ks > k\int r$ seu $s > \int r$. Quare si in fractione $\frac{r}{s}$ fuerit $s = \int r$, erit $z = r$; sin autem sit $s > \int r$, erit z aequale multiplo cuipiam ipsius r. Unde patet, si sit $s < \int r$, aequationem $\frac{z}{\int z} = \frac{r}{s}$ esse impossibilem neque hoc casu numeros amicabiles inveniri posse. Deinde cum sit

$$\frac{\int z}{z} = \frac{na+mb}{n\int a} - \frac{a+b}{nx\int a} = \frac{a}{\int a} + \frac{b}{\int b} - \frac{a+b}{nx\int a},$$

1) Editio princeps (atque etiam *Comment. arithm.*): *divisores ipsius r.* Correxit F. R.

ob $\frac{a}{\int a} < 1$ et $\frac{b}{\int b} < 1$ erit $\frac{\int z}{z} < 2 - \frac{a+b}{nx\int a}$[1]) ideoque multo magis $\frac{z}{\int z} > \frac{1}{2}$, ita ut z sit semper numerus deficiens. Hincque patet aequationem $\frac{z}{\int z} = \frac{r}{s}$ semper ita fore comparatam, ut sit $\frac{r}{s} > \frac{1}{2}$ seu $s < 2r$. Unde si sit $\int r = s$, erit $\int r < 2r$, et si $s > \int r$, erit multo magis $\int r < 2r$. Utroque igitur casu r erit numerus deficiens. Quocirca si x tanquam numerus incognitus spectetur, proposita aequatione $\frac{z}{\int z} = \frac{nx\int a}{(na+mb)x-a-b}$ valorem ipsius x ita determinari oportet, ut reducta fractione $\frac{nx\int a}{(na+mb)x-a-b}$ ad minimos terminos $\frac{r}{s}$ fiat r numerus deficiens et ut sit vel $s = \int r$ vel $s > \int r$.

Quibus conditionibus animadversis tam r quam s in suos factores simplices primos resolvatur, ut prodeat huiusmodi aequatio

$$\frac{z}{\int z} = \frac{A^\alpha B^\beta C^\gamma}{E^\varepsilon F^\zeta G^\eta};$$

tunc autem successive vel A^α vel altior potestas ipsius A ponatur factor ipsius z seu ponatur $z = P\cdot A^{\alpha+\nu}$; erit $\int z = \int A^{\alpha+\nu}\cdot\int P$ et $\frac{z}{\int z} = \frac{PA^{\alpha+\nu}}{\int A^{\alpha+\nu}\cdot\int P}$ ideoque

$$\frac{P}{\int P} = \frac{B^\beta C^\gamma \int A^{\alpha+\nu}}{A^\nu E^\varepsilon F^\zeta G^\eta}.$$

Similique modo ponatur ulterius $P = B^{\beta+\mu}Q$ et hoc pacto procedatur, donec tandem perveniatur ad aequationem huius formae $\frac{Z}{\int Z} = \frac{u}{\int u}$, ex qua habeatur $Z = u$. Saepe quidem haec operatio successu optato caret, sed pro quovis casu oblato facilius erit operationem hanc per exempla docere quam per praecepta.

EXEMPLUM 1

109. Sit $a = 3$, $b = 1$; erit $\int a = 4$, $\int b = 1$ et $m = 4$, $n = 1$ ac numeri amicabiles erunt

$$3(x-1)z \quad \text{et} \quad (4x-1)z,$$

1) In editione principe (nec non in *Comment. arithm.*) hic et in priori formula $a-b$ loco $a+b$ scriptum est. Correxit F. R.

si sint $x-1$ et $4x-1$ numeri primi et

$$\frac{z}{\int z}=\frac{4x}{7x-4}.$$

Hic autem primo patet, si 4 ex numeratore non tollatur, fore $7x-4<\int 4x$ ob $\int 4x=7\int x$. Ergo necesse est, ut sit $7x-4$ numerus par. Ponatur $x=4p$; erit

$$\frac{z}{\int z}=\frac{4p}{7p-1}.$$

Nunc fiat $7p-1$ numerus par ponendo $p=2q+1$; erit

$$\frac{z}{\int z}=\frac{2(2q+1)}{7q+3}$$

et $x=8q+4$ atque

$$x-1=8q+3,\quad 4x-1=32q+15.$$

Unde q nequit esse multiplum ternarii, ne $x-1$ fiat per 3 divisibile. Erit ergo vel $q=3r+1$ vel $q=3r-1$; priori casu fit $2q+1=6r+3$ ac z deberet esse divisibile per 3, quod pariter fieri nequit, quia in altero numero quaesito $3(x-1)z$ iam inest factor 3. Sit igitur $q=3r-1$; erit

$$\frac{z}{\int z}=\frac{2(6r-1)}{21r-4}$$

atque $x=24r-4$,

$$x-1=24r-5\quad\text{et}\quad 4x-1=96r-17.$$

Cum autem z factorem 3 habere nequeat, nisi binarius ex numeratore $2(6r-1)$ tollatur, z erit divisibile per 2 et posito $z=2y$ fieret

$$\frac{2y}{3\int y}=\frac{2(6r-1)}{21r-4}\quad\text{et}\quad\frac{y}{\int y}=\frac{3(6r-1)}{21r-4}$$

ideoque evaderet y et propterea quoque z per 3 divisibile, quod fieri nequit. Hanc ob rem iste binarius ex numeratore tolli debet ponendo $r=2s$, ut sit

$$x-1=48s-5,\quad 4x-1=192s-17,$$

eritque

$$\frac{z}{\int z}=\frac{12s-1}{21s-2}.$$

Iam si s sit numerus impar, ob z numerum imparem fiet quoque $\int z = k(21s-2)$ numerus impar, ex quo sequitur numerum z fore quadratum; sin autem s sit numerus par, factor communis z non erit quadratus. Evolvantur ergo ii ipsius s valores, qui efficiunt $x-1=48s-5$ et $4x-1=192s-17$ numeros primos, et dispiciatur, utrum aequationi $\frac{z}{\int z}=\frac{12s-1}{21s-2}$ satisfieri queat.

Sit $s=7$; erit $x-1=331$, $4x-1=1327$ et $\frac{z}{\int z}=\frac{83}{145}$. Iam cum z debeat esse quadratum, ponatur $z=83^2A$; erit $\int z=367\cdot 19\int A$ et $\frac{A}{\int A}=\frac{367\cdot 19}{5\cdot 29\cdot 83}$. Nunc autem ipsius A factor statui nequit 19^2 ob $\int 19^2=3\cdot 127$; prodiret enim 3 factor ipsius A; altioribus vero potestatibus sumendis mox devenitur ad numeros tam grandes, ut facile pateat opus succedere non posse.

Sit $s=12$; erit $x-1=571$, $4x-1=2287$ et $\frac{z}{\int z}=\frac{11\cdot 13}{2\cdot 125}$, quae neque 11^2 neque 13 pro factoribus ipsius z assumendo resolvi potest.

Neque vero etiam ex maioribus valoribus pro s mihi quicquam praestare licuit.

EXEMPLUM 2

110. Sit $a=5$, $b=1$; erit $\int a=6$, $\int b=1$, $m=6$, $n=1$ et numeri amicabiles erunt

$$5(x-1)z \quad \text{et} \quad (6x-1)z$$

habebiturque

$$\frac{z}{\int z}=\frac{6x}{11x-6}.$$

Quae aequatio ut sit possibilis, ex numeratore $6x$ vel binarium vel ternarium tollere oportet, quia alioquin numerator maneret numerus redundans. Habebimus ergo duos casus evolvendos.

I. Tollatur ex numeratore ternarius ponendo $x=3p$; erit

$$\frac{z}{\int z}=\frac{6p}{11p-2};$$

nunc vero porro ponatur $p=3q+1$ eritque

$$\frac{z}{\int z}=\frac{2(3q+1)}{11q+3}$$

et ob $x = 9q + 3$ numeri primi esse debent

$$x - 1 = 9q + 2 \quad \text{et} \quad 6x - 1 = 54q + 17,$$

ubi patet q esse debere numerum imparem. Sit ergo $q = 2r - 1$; erit

$$x - 1 = 18r - 7, \quad 6x - 1 = 108r - 37 \quad \text{et} \quad \frac{z}{\int z} = \frac{2(6r-2)}{22r-8} = \frac{2(3r-1)}{11r-4}.$$

Evolvantur iam casus, quibus $18r - 7$ et $108r - 37$ fiunt numeri primi, qui sunt:

1) $r = 1$; erit

$$x - 1 = 11, \quad 6x - 1 = 71 \quad \text{et} \quad \frac{z}{\int z} = \frac{2 \cdot 2}{7} = \frac{4}{7}.$$

Cum igitur hic sit $7 = \int 4$, erit $z = 4$ et numeri amicabiles erunt

$$\begin{cases} 4 \cdot 5 \cdot 11 \\ 4 \cdot 71, \end{cases}$$

quos quidem iam invenimus.

2) $r = 2$; erit

$$x - 1 = 29, \quad 6x - 1 = 179 \quad \text{et} \quad \frac{z}{\int z} = \frac{2 \cdot 5}{2 \cdot 9} = \frac{5}{9}.$$

At z factorem 5 habere nequit.

3) $r = 5$; erit

$$x - 1 = 83, \quad 6x - 1 = 503 \quad \text{et} \quad \frac{z}{\int z} = \frac{4 \cdot 7}{3 \cdot 17};$$

at hic $3 \cdot 17 < \int 4 \cdot 7$.

4) $r = 8$; erit

$$x - 1 = 137, \quad 6x - 1 = 827 \quad \text{et} \quad \frac{z}{\int z} = \frac{23}{2 \cdot 3 \cdot 7}.$$

Ponatur $z = 23P$; erit

$$\int z = 24 \int P \quad \text{et} \quad \frac{P}{\int P} = \frac{24}{23} \cdot \frac{z}{\int z} = \frac{4}{7},$$

unde $P = 4$ et $z = 4 \cdot 23$, quam operationem ita breviter repraesento

$$\frac{z}{\int z} = \frac{23}{2 \cdot 3 \cdot 7} \boxed{\frac{23}{24}} \frac{4}{7} \boxed{\frac{4}{7}};$$

unde fit $z = 4 \cdot 23$ et numeri amicabiles erunt

$$\begin{cases} 4 \cdot 23 \cdot 5 \cdot 137 \\ 4 \cdot 23 \cdot 827. \end{cases}$$

Reliqui valores, quousque quidem examinavi, nullos dant numeros amicabiles.

II. Tollatur ex numeratore binarius ponendo $x = 2p$; erit

$$\frac{z}{\int z} = \frac{6p}{11p-3}.$$

Nunc sit $p = 2q + 1$; erit

$$\frac{z}{\int z} = \frac{3(2q+1)}{11q+4}$$

et numeri primi esse debebunt ob $x = 4q + 2$

$$x - 1 = 4q + 1, \quad 6x - 1 = 24q + 11;$$

quare esse nequit $q = 3\alpha - 1$. Deinde cum z non esse debeat divisibile per 5, neque $2q + 1$ neque $4q + 1$ neque $24q + 11$ per 5 debet esse divisibile, unde excluduntur casus $q = 5\alpha + 2$, $q = 5\alpha + 1$. Reiectis ergo his aliisque valoribus inutilibus ipsius q, qui pro $x - 1$ et $6x - 1$ non praebent numeros primos, calculus ita se habebit:

q	$x-1$	$6x-1$	$\frac{z}{\int z}$
3	13	83	$\frac{3 \cdot 7}{37}$ nihil dat.
4	17	107	$\frac{3 \cdot 9}{48} = \frac{9}{16}\boxed{\frac{9}{13}}\frac{13}{16}\boxed{\frac{13}{14}}\frac{7}{8}\boxed{\frac{7}{8}}$, $\quad z = 9 \cdot 7 \cdot 13$,
			vel $\frac{9}{16}\boxed{\frac{27}{40}}\frac{5}{6}\boxed{\frac{5}{6}}$, ergo $z = 27 \cdot 5$; hic autem valor ob
			$a = 5$ est inutilis.
			Erunt ergo numeri amicabiles
			$\begin{cases} 9 \cdot 7 \cdot 13 \cdot 5 \cdot 17 \\ 9 \cdot 7 \cdot 13 \cdot 107. \end{cases}$

q	$x-1$	$6x-1$	$\dfrac{z}{\int z}$
9	37	227	$\dfrac{3\cdot 19}{103}$ nihil dat.
10	41	251	$\dfrac{3\cdot 21}{114} = \dfrac{3\cdot 7}{2\cdot 19} \Big\vert \dfrac{7^2}{3\cdot 19} \quad \dfrac{3^2}{2\cdot 7} \quad \dfrac{3^2}{13} \quad \dfrac{13}{14} \quad \dfrac{13}{14}$. Ergo $z = 3^2\cdot 7^2\cdot 13$ et numeri amicabiles erunt $\begin{cases} 3^2\cdot 7^2\cdot 13\cdot 5\cdot 41 \\ 3^2\cdot 7^2\cdot 13\cdot 251. \end{cases}$
18	73	443	$\dfrac{3\cdot 37}{202} = \dfrac{3\cdot 37}{2\cdot 101}$ nihil dat.
24	97	587	$\dfrac{3\cdot 49}{268} = \dfrac{3\cdot 49}{4\cdot 67}$ nihil dat.
28	113	683	$\dfrac{3\cdot 57}{312} = \dfrac{9\cdot 19}{8\cdot 39} = \dfrac{3\cdot 19}{8\cdot 13}$ nihil dat.
34	137	827	$\dfrac{3\cdot 69}{378} = \dfrac{23}{2\cdot 21} = \dfrac{23}{2\cdot 3\cdot 7} \Big\vert \dfrac{23}{24} \Big\vert \dfrac{4}{7} \Big\vert \dfrac{4}{7}$, $z = 4\cdot 23$ ut ante.
39	157	947	$\dfrac{3\cdot 79}{483}$ nihil dat.
45	181	1091	$\dfrac{3\cdot 91}{499} = \dfrac{3\cdot 7\cdot 13}{499}$
48	193	1163	$\dfrac{3\cdot 97}{532} = \dfrac{3\cdot 97}{4\cdot 7\cdot 19} = \dfrac{3\cdot 97}{4\cdot 133} \Big\vert \dfrac{97}{2\cdot 7^2} \Big\vert \dfrac{3\cdot 7}{2\cdot 19} \quad \dfrac{7^2}{3\cdot 19} \Big\vert \dfrac{3^2}{2\cdot 7} \Big\vert \dfrac{3^2}{13} \Big\vert \dfrac{13}{14} \Big\vert \dfrac{13}{14}$. Ergo $z = 3^2\cdot 7^2\cdot 13\cdot 97$ et numeri amicabiles sunt $\begin{cases} 3^2\cdot 7^2\cdot 13\cdot 97\cdot 5\cdot 193 \\ 3^2\cdot 7^2\cdot 13\cdot 97\cdot 1163. \end{cases}$
49	197	1187	$\dfrac{3\cdot 99}{543} = \dfrac{9\cdot 11}{181}$
60	241	1451	$\dfrac{3\cdot 121}{664} = \dfrac{3\cdot 11^2}{8\cdot 83}$

q	$x-1$	$6x-1$	$\frac{z}{\int z}$
69	277	1667	$\frac{3\cdot 139}{763}$
79	317	1907	$\frac{3\cdot 159}{873}=\frac{53}{97}$
84	337	2027	$\frac{3\cdot 169}{928}=\frac{3\cdot 169}{8\cdot 116}=\frac{3\cdot 169}{32\cdot 29}$
93	373	2243	$\frac{3\cdot 187}{1027}=\frac{3\cdot 11\cdot 17}{13\cdot 79}$
100	401	2411	$\frac{3\cdot 201}{1104}=\frac{3\cdot 67}{368}=\frac{3\cdot 67}{16\cdot 23}$
244	977	5867	$\frac{3\cdot 489}{2688}=\frac{3\cdot 163}{128\cdot 7}\boxed{\frac{163}{4\cdot 41}}\frac{3\cdot 41}{32\cdot 7}\boxed{\frac{41}{2\cdot 3\cdot 7}}\frac{3^2}{16}\boxed{\frac{3^2}{13}}\frac{13}{16}\boxed{\frac{13}{14}}\frac{7}{8}\boxed{\frac{7}{8}}.$

Ergo $z=3^2\cdot 7\cdot 13\cdot 41\cdot 163$ et numeri amicabiles erunt

$$\begin{cases}3^2\cdot 7\cdot 13\cdot 41\cdot 163\cdot 5\cdot 977\\ 3^2\cdot 7\cdot 13\cdot 41\cdot 163\cdot 5867.\end{cases}$$

Hinc ergo bini prodierunt novi numeri amicabiles.

EXEMPLUM 3

111. Sit $a=7$, $b=1$; erit $\int a=8$, $\int b=1$, $m=8$, $n=1$ et numeri amicabiles

$$7(x-1)z \quad \text{et} \quad (8x-1)z$$

existente

$$\frac{z}{\int z}=\frac{8x}{15x-8}.$$

Ac primo quidem x debet esse numerus par; ponatur ergo $x=2p$; erit

$$x-1=2p-1, \quad 8x-1=16p-1$$

et

$$\frac{z}{\int z}=\frac{8p}{15p-4},$$

quae aequatio est impossibilis, nisi potestas binarii in numeratore deprimatur, quia $15p-4<\int 8p$. Ergo fiat $p=4q$, ut sit

$$x=8q, \quad x-1=8q-1, \quad 8x-1=64q-1$$

et

$$\frac{z}{\int z}=\frac{8q}{15q-1}.$$

Nunc sit $q = 2r + 1$; erit

$$\frac{z}{\int z} = \frac{4(2r+1)}{15r+7}$$

et

$$x - 1 = 16r + 7, \quad 8x - 1 = 128r + 63;$$

quorum numerorum ut neuter sit per 3 divisibilis, neque erit $r = 3\alpha - 1$ neque $r = 3\alpha$. Sit ergo $r = 3s + 1$; erit

$$\frac{z}{\int z} = \frac{4(6s+3)}{45s+22} \quad \text{seu} \quad \frac{z}{\int z} = \frac{4 \cdot 3(2s+1)}{45s+22}$$

et

$$x - 1 = 48s + 23, \quad 8x - 1 = 384s + 191.$$

Nunc vel ternarius vel quaternarius ex numeratore tolli debet. At ternarius tolli nequit, quia denominator nunquam per 3 est divisibilis; tollatur ergo quaternarius, ad quod pono $s = 2t$, eritque

$$\frac{z}{\int z} = \frac{2 \cdot 3(4t+1)}{45t+11};$$

nunc sit $t = 2u - 1$; erit

$$\frac{z}{\int z} = \frac{3(8u-3)}{45u-17};$$

at est $s = 4u - 2$ ideoque numeri primi esse debent

$$x - 1 = 192u - 73, \quad 8x - 1 = 1536u - 577.$$

u	$x-1$	$8x-1$	$\frac{z}{\int z}$
5	887	7103	$\frac{3 \cdot 37}{208} = \frac{3 \cdot 37}{16 \cdot 13} \boxed{\frac{37}{2 \cdot 19}} \frac{3 \cdot 19}{8 \cdot 13} \boxed{\frac{19}{4 \cdot 5}} \frac{3 \cdot 5}{2 \cdot 13} \boxed{\frac{5}{2 \cdot 3}} \frac{3^2}{13} \boxed{\frac{3^2}{13}}$. Ergo $z = 3^2 \cdot 5 \cdot 19 \cdot 37$ et numeri amicabiles erunt $\begin{cases} 3^2 \cdot 5 \cdot 19 \cdot 37 \cdot 7 \cdot 887 \\ 3^2 \cdot 5 \cdot 19 \cdot 37 \cdot 7103. \end{cases}$
11	2039	16319	$\frac{3 \cdot 5 \cdot 17}{2 \cdot 239}$
13	2423	19391	$\frac{3 \cdot 101}{8 \cdot 71}$
26	4919	39359	$\frac{3 \cdot 205}{1153}$.

EXEMPLUM 4

112. Sit $a = 11$, $b = 1$; erit $\int a = m = 12$, $\int b = n = 1$, numeri quaesiti

$$11(x-1)z \quad \text{et} \quad (12x-1)z$$

atque

$$\frac{z}{\int z} = \frac{12x}{23x-12}.$$

Hic ex numeratore vel 3 vel 4 tolli debet.

I. Tollatur 3; ponatur $x = 3p$, erit

$$\frac{z}{\int z} = \frac{12p}{23p-4},$$

et $p = 3q - 1$; erit

$$\frac{z}{\int z} = \frac{4(3q-1)}{23q-9}$$

et ob $x = 9q - 3$ q debet esse impar. Sit $q = 2r + 1$, ut sit $x = 18r + 6$; erit

$$\frac{z}{\int z} = \frac{4(6r+2)}{46r+14} = \frac{4(3r+1)}{23r+7}$$

et

$$x - 1 = 18r + 5, \quad 12x - 1 = 216r + 71.$$

r	$x-1$	$12x-1$	$\frac{z}{\int z}$
0	5	71	$\frac{4}{7}$, $z = 4$; numeri amicabiles $\begin{cases} 4 \cdot 11 \cdot 5 \\ 4 \cdot 71. \end{cases}$
2	41	503	$\frac{4 \cdot 7}{53}$
3	59	719	$\frac{4 \cdot 10}{76} = \frac{2 \cdot 5}{19}$ impossibile.
6	113	1367	$\frac{4 \cdot 19}{145} = \frac{4 \cdot 19}{5 \cdot 29}$ impossibile.
7	131	1583	$\frac{4 \cdot 22}{168} = \frac{11}{21} = \frac{11}{3 \cdot 7} \boxed{\frac{11}{12}} \frac{4}{7} \boxed{\frac{4}{7}}$, sed ob factorem 11 hic valor z non valet.

II. Tollatur factor 4 ac ponatur $x = 4p$, ut fiat

$$\frac{z}{\int z} = \frac{12p}{23p-3}.$$

Iam sit $p = 4q + 1$; erit

$$\frac{z}{\int z} = \frac{3(4q+1)}{23q+5}$$

et ob $x = 16q + 4$ numeri primi esse debent

$$x - 1 = 16q + 3 \quad \text{et} \quad 12x - 1 = 192q + 47;$$

hinc excluduntur valores $q = 3\alpha$.

q	$x-1$	$12x-1$	$\frac{z}{\int z}$
0	3	47	$\frac{3}{5}$ impossibile.
1	19	239	$\frac{3\cdot5}{4\cdot7} \Big\vert \frac{5}{2\cdot3} \; \frac{3^2}{14} \Big\vert \frac{3^2}{13} \Big\vert \frac{13}{14} \Big\vert \frac{13}{14}$; $z = 3^2\cdot5\cdot13$ et numeri amicabiles erunt $\begin{cases} 3^2\cdot5\cdot13\cdot11\cdot19 \\ 3^2\cdot5\cdot13\cdot239. \end{cases}$
13	211	2543	$\frac{3\cdot53}{16\cdot19} \Big\vert \frac{53}{2\cdot27} \Big\vert \frac{81}{8\cdot19} \Big\vert \frac{243}{4\cdot7\cdot13} \Big\vert \frac{7\cdot13}{2\cdot3\cdot19} \Big\vert \frac{13}{2\cdot7} \Big\vert \frac{7^2}{3\cdot19} \Big\vert \frac{7^2}{3\cdot19}$. Ergo $z = 3^5\cdot7^2\cdot13\cdot53$ et numeri amicabiles erunt $\begin{cases} 3^5\cdot7^2\cdot13\cdot53\cdot11\cdot211 \\ 3^5\cdot7^2\cdot13\cdot53\cdot2543. \end{cases}$

EXEMPLUM 5

113. Sit $a = 5$, $b = 17$ et numeri amicabiles

$$5(3x-1)z \quad \text{et} \quad 17(x-1)z;$$

erit

$$\frac{z}{\int z} = \frac{18x}{32x-22} = \frac{9x}{16x-11}.$$

Cum x debeat esse numerus par, ponatur $x = 2p$; erit

$$\frac{z}{\int z} = \frac{18p}{32p-11}$$

et ex numeratore $18p$ vel factor 2 vel 3^2 tolli debet, ne sit numerus redundans. At factor 2 tolli nequit; tollatur ergo factor 9. Ad hoc ponatur $p = 9q + 4$, ut sit $x = 18q + 8$ et

$$x - 1 = 18q + 7 \quad \text{et} \quad 3x - 1 = 54q + 23;$$

erit

$$\frac{z}{\int z} = \frac{2(9q+4)}{32q+13}.$$

q	$x-1$	$3x-1$	$\frac{z}{\int z}$
0	7	23	$\frac{8}{13}$ impossibile.
2	43	131	$\frac{4\cdot 11}{7\cdot 11} = \frac{4}{7}$; $z = 4$ et numeri amicabiles $\begin{cases} 4\cdot 5\cdot 131 \\ 4\cdot 17\cdot 43. \end{cases}$
4	79	239	$\frac{16\cdot 5}{3\cdot 47}$
5	97	293	$\frac{2\cdot 49}{173}$
17	313	941	$\frac{2\cdot 157}{557}$
19	349	1049	$\frac{2\cdot 5^2\cdot 7}{27\cdot 23}$
20	367	1103	$\frac{16\cdot 23}{653}$
24	439	1319	$\frac{8.5\cdot 11}{781}$ inutile, $= \frac{8\cdot 5}{71}$.

EXEMPLUM 6

114. Sit $a = 37$ et $b = 227$; erit $\int a = 38$, $\int b = 228$ et $\frac{m}{n} = \frac{1}{6}$; unde si numeri amicabiles sint

$$37(6x-1)z \quad \text{et} \quad 227(x-1)z,$$

fiet

$$\frac{z}{\int z} = \frac{6\cdot 38x}{449x - 264} = \frac{4\cdot 3\cdot 19x}{449x-264}.$$

Ubi cum x debeat esse numerus par, ponatur $x = 2p$, ut numeri primi esse

debeant

$$x-1=2p-1 \quad \text{et} \quad 6x-1=12p-1,$$

eritque

$$\frac{z}{\int z}=\frac{4\cdot 3\cdot 19p}{449p-132}.$$

Nunc ex numeratore vel factor 4 vel factor 3 tolli debet.

I. Tollatur factor 3; ad hoc ponatur $p=3q$, ut sit

$$\frac{z}{\int z}=\frac{4\cdot 3\cdot 19q}{449q-44};$$

nunc fiat $q=3r+1$ eritque

$$\frac{z}{\int z}=\frac{4\cdot 19(3r+1)}{449r+135}$$

et $p=9r+3$ et

$$x-1=18r+5, \quad 6x-1=108r+35.$$

r	$x-1$	$6x-1$	$\frac{z}{\int z}$
2	41	251	$\frac{4\cdot 19\cdot 7}{1033}$
3	59	359	$\frac{4\cdot 19\cdot 10}{1482}=\frac{4\cdot 5}{3\cdot 13}$
6	113	683	$\frac{4\cdot 19\cdot 19}{3\cdot 23\cdot 41}$
13	239	1439	$\frac{4\cdot 19\cdot 40}{4\cdot 1493}$
17	311	1871	$\frac{16\cdot 13\cdot 19}{8\cdot 971}$
22	401	2411	$\frac{4\cdot 19\cdot 67}{10013}=\frac{4\cdot 67}{17\cdot 31}\ \boxed{\frac{67}{4\cdot 17}}\ \frac{16}{31}\ \boxed{\frac{16}{31}};$
			$z=16\cdot 67$ et numeri amicabiles $\begin{cases}16\cdot 67\cdot 37\cdot 2411\\ 16\cdot 67\cdot 227\cdot 401.\end{cases}$
117	2111	12671	$\frac{4\cdot 19\cdot 352}{52668}=\frac{128\cdot 11\cdot 19}{4\cdot 7\cdot 9\cdot 11\cdot 19}=\frac{32}{63};$
			$z=32$ et numeri amicabiles $\begin{cases}32\cdot 37\cdot 12671\\ 32\cdot 227\cdot 2111.\end{cases}$

II. Tollatur factor 4; ponatur $p = 4q$; erit

$$\frac{z}{\int z} = \frac{4\cdot 3\cdot 19q}{449q - 33};$$

nunc sit $q = 4r + 1$; erit $p = 16r + 4$ et

$$x - 1 = 32r + 7, \quad 6x - 1 = 192r + 47$$

atque

$$\frac{z}{\int z} = \frac{3\cdot 19(4r+1)}{449r + 104}.$$

r	$x-1$	$6x-1$	$\frac{z}{\int z}$
0	7	47	$\frac{3\cdot 19}{8\cdot 13}\ \boxed{\frac{19}{4\cdot 5}}\ \frac{3\cdot 5}{2\cdot 13}\ \boxed{\frac{5}{2\cdot 3}}\ \frac{3^2}{13}\ \boxed{\frac{3^2}{13}};$ $z = 3^2\cdot 5\cdot 19$ et numeri amicabiles $\begin{cases} 3^2\cdot 5\cdot 19\cdot 37\cdot 47 \\ 3^2\cdot 5\cdot 19\cdot 227\cdot 7. \end{cases}$
2	71	431	$\frac{9\cdot 19}{2\cdot 167}$
8	263	1583	$\frac{3\cdot 19\cdot 33}{16\cdot 3\cdot 7\cdot 11} = \frac{3\cdot 19}{16\cdot 7}\ \boxed{\frac{19}{4\cdot 5}}\ \frac{3\cdot 5}{4\cdot 7}\ \boxed{\frac{5}{2\cdot 3}}\ \frac{3^2}{2\cdot 7}\ \boxed{\frac{3^2}{13}}\ \frac{13}{14}\ \boxed{\frac{13}{14}};$ $z = 3^2\cdot 5\cdot 13\cdot 19$ et numeri amicabiles $\begin{cases} 3^2\cdot 5\cdot 13\cdot 19\cdot 37\cdot 1583 \\ 3^2\cdot 5\cdot 13\cdot 19\cdot 227\cdot 263. \end{cases}$
15	487	2927	$\frac{3\cdot 19\cdot 61}{7\cdot 977}$
23	743	4463	$\frac{9\cdot 19\cdot 31}{9\cdot 19\cdot 61} = \frac{31}{61}$
26	839	5039	$\frac{3\cdot 19\cdot 105}{2\cdot 3\cdot 13\cdot 151} = \frac{3\cdot 5\cdot 7\cdot 19}{2\cdot 13\cdot 151}$
30	967	5807	$\frac{3\cdot 19\cdot 11}{2\cdot 617}$
41	1319	7919	$\frac{3\cdot 19\cdot 165}{9\cdot 121\cdot 17} = \frac{5\cdot 19}{11\cdot 17}.$

EXEMPLUM 7

115. Sit $a = 79$, $b = 11 \cdot 19 = 209$, $\int a = 80$, $\int b = 240$; erit $m = 1$, $n = 3$ et numeri amicabiles sint

$$79(3x-1)z \quad \text{et} \quad 11 \cdot 19(x-1)z;$$

erit

$$\frac{z}{\int z} = \frac{240x}{446x-288} = \frac{120x}{223x-144}.$$

Sit $x = 2p$; erit

$$\frac{z}{\int z} = \frac{120p}{223p-72}$$

et numeri primi esse debent $2p-1$ et $6p-1$. Nunc autem ex numeratore $120p$ vel factor 8 vel 3 tolli debet.

I. Tollatur factor 3; sit $p = 9q$; erit

$$\frac{z}{\int z} = \frac{120q}{223q-8}$$

et fiat $q = 3r-1$, ut sit

$$\frac{z}{\int z} = \frac{40(3r-1)}{223r-77},$$

$p = 27r-9$ et

$$x-1 = 54r-19 \quad \text{ac} \quad 3x-1 = 162r-55.$$

Nunc autem ob 40 numerum redundantem vel 5 vel 4 tolli debet.

α) Tollatur 5 sitque $r = 5s-1$; erit

$$\frac{z}{\int z} = \frac{8(15s-4)}{223s-60}$$

et numeros primos esse oportet $x-1 = 270s-73$, $3x-1 = 810s-217$. Ac ne ternarius denuo in numeratorem intret, excludendi sunt casus $s = 3\alpha-1$.[1]) Hinc autem nihil invenitur.

β) Cum sit $\frac{z}{\int z} = \frac{40(3r-1)}{223r-77}$, tollatur 4 sitque $r = 4s-1$; erit

$$\frac{z}{\int z} = \frac{10(12s-4)}{223s-75} = \frac{40(3s-1)}{223s-75};$$

1) Observandum quidem est numeratorem nunquam per 3 divisibilem esse. F. R.

sit porro $s = 4t + 1$; erit

$$\frac{z}{\int z} = \frac{10(12t+2)}{223t+37} = \frac{20(6t+1)}{223t+37}.$$

Sit porro $t = 2u - 1$; erit

$$\frac{z}{\int z} = \frac{10(12u-5)}{223u-93}$$

et ob $r = 16t + 3 = 32u - 13$ erit $x - 1 = 1728u - 721$, $3x - 1 = 5184u - 2161$. At hos numeros non reddit primos minor valor ipsius u quam 16, unde fit $\frac{z}{\int z} = \frac{2\cdot 11\cdot 17}{5\cdot 139}$, qui ob factorem 11 est inutilis.

II. Ergo ex aequatione $\frac{z}{\int z} = \frac{120p}{223p - 72}$ tollatur factor 8. Ponatur $p = 8q$; erit

$$\frac{z}{\int z} = \frac{120q}{223q - 9}$$

et nunc sit $q = 8r - 1$; erit

$$\frac{z}{\int z} = \frac{3\cdot 5(8r-1)}{223r-29};$$

at ob $p = 64r - 8$ erit

$$x - 1 = 128r - 17, \quad 3x - 1 = 384r - 49.$$

Unde valores exluduntur $r = 3\alpha + 1$ et $r = 5\alpha + 1$.

r	$x-1$	$3x-1$	$\frac{z}{\int z}$
2	239	719	$\frac{3\cdot 5^2}{139}$
3	367	1103	$\frac{3\cdot 23}{128}\ \boxed{\frac{23}{8\cdot 3}}\ \frac{3^2}{16}\ \boxed{\frac{3^2}{13}}\ \frac{13}{16}\ \boxed{\frac{13}{14}}\ \frac{7}{8}\ \boxed{\frac{7}{8}}$, ergo $z = 3^2\cdot 7\cdot 13\cdot 23$, vel
			$\frac{3\cdot 23}{128}\ \boxed{\frac{23}{8\cdot 3}}\ \frac{3^2}{16}\ \boxed{\frac{3^3}{8\cdot 5}}\ \frac{5}{6}\ \boxed{\frac{5}{6}}$, ergo $z = 3^3\cdot 5\cdot 23$,

et numeri amicabiles erunt

$$\begin{cases} 3^2\cdot 7\cdot 13\cdot 23\cdot 79\cdot 1103 \\ 3^2\cdot 7\cdot 13\cdot 23\cdot 11\cdot 19\cdot 367 \end{cases} \quad \text{vel} \quad \begin{cases} 3^3\cdot 5\cdot 23\cdot 79\cdot 1103 \\ 3^3\cdot 5\cdot 23\cdot 11\cdot 19\cdot 367. \end{cases}$$

EXEMPLUM 8

116. Sit $a = 17 \cdot 19$, $b = 11 \cdot 59$; erit $\int a = 18 \cdot 20$, $\int b = 12 \cdot 60$ et $m = 1$, $n = 2$. Si ergo numeri amicabiles ponantur

$$17 \cdot 19(2x - 1)z, \quad 11 \cdot 59(x - 1)z,$$

erit

$$\frac{z}{\int z} = \frac{720x}{1295x - 972}.$$

Sit $x = 2p$; erit

$$\frac{z}{\int z} = \frac{720p}{1295p - 486}$$

atque

$$x - 1 = 2p - 1, \quad 2x - 1 = 4p - 1;$$

quorum ut neuter sit divisibilis per 3, debet esse $p = 3q$, ut sit

$$\frac{z}{\int z} = \frac{720q}{1295q - 162}$$

et

$$x - 1 = 6q - 1, \quad 2x - 1 = 12q - 1.$$

Tollatur ex numeratore factor 16 sitque $q = 2r$; erit

$$\frac{z}{\int z} = \frac{720r}{1295r - 81};$$

nunc sit $r = 16s - 1$; erit

$$\frac{z}{\int z} = \frac{45(16s - 1)}{1295s - 86}$$

et

$$x - 1 = 192s - 13, \quad 2x - 1 = 384s - 25.$$

Sit $s = 1$; erit $x - 1 = 179$, $2x - 1 = 359$ et

$$\frac{z}{\int z} = \frac{45 \cdot 15}{1209} = \frac{225}{403} = \frac{3^2 \cdot 5^2}{13 \cdot 31} \left|\frac{3^2}{13}\right| \frac{5^2}{31} \left|\frac{5^2}{31}\right|.$$

Ergo $z = 3^2 \cdot 5^2$ et numeri amicabiles erunt

$$\begin{cases} 3^2 \cdot 5^2 \cdot 17 \cdot 19 \cdot 359 \\ 3^2 \cdot 5^2 \cdot 11 \cdot 59 \cdot 179. \end{cases}$$

SCHOLION

117. Haec ultima methodus in Problemate 5 exposita prorsus diversa est a methodo praecedente, quam problemata quatuor priora complectuntur: dum in hac factor communis quaeritur, in illa autem datur. Utraque tamen singulari praestantiae genere est praedita, ut altera sine subsidio alterius non satis apta sit ad multitudinem numerorum amicabilium augendam. Posterior enim methodus suppeditat eiusmodi factores communes, quos ad usum prioris vix suspicari licuisset, prior vero suggerit reliquos factores huic instituto idoneos. Ceterum cuncta, quae hic tradidi, specimen continent methodi summae incertae, quam, quantum licuit, ad regulas algebraicas reduxi, ut vaga tentandi incertitudo restringeretur. Coronidis ergo loco ultra sexaginta numerorum amicabilium paria subiungam, quos his methodis elicui.

CATALOGUS NUMERORUM AMICABILIUM

$$\text{I. } \begin{cases} 2^2\cdot 5\cdot 11 \\ 2^2\cdot 71 \end{cases} \qquad \text{II. } \begin{cases} 2^4\cdot 23\cdot 47 \\ 2^4\cdot 1151 \end{cases}$$

$$\text{III. } \begin{cases} 2^7\cdot 191\cdot 383 \\ 2^7\cdot 73727 \end{cases} \qquad \text{IV. } \begin{cases} 2^2\cdot 23\cdot 5\cdot 137 \\ 2^2\cdot 23\cdot 827 \end{cases}$$

$$\text{V. } \begin{cases} 3^2\cdot 7\cdot 13\cdot 5\cdot 17 \\ 3^2\cdot 7\cdot 13\cdot 107 \end{cases} \qquad \text{VI. } \begin{cases} 3^2\cdot 5\cdot 13\cdot 11\cdot 19 \\ 3^2\cdot 5\cdot 13\cdot 239 \end{cases}$$

$$\text{VII. } \begin{cases} 3^2\cdot 7^2\cdot 13\cdot 5\cdot 41 \\ 3^2\cdot 7^2\cdot 13\cdot 251 \end{cases} \qquad \text{VIII. } \begin{cases} 3^2\cdot 5\cdot 7\cdot 53\cdot 1889 \\ 3^2\cdot 5\cdot 7\cdot 102059 \end{cases}$$

$$\text{IX. } \begin{cases} 2^2\cdot 13\cdot 17\cdot 389\cdot 509 \\ 2^2\cdot 13\cdot 17\cdot 198899 \end{cases} \qquad \text{X. } \begin{cases} 3^2\cdot 5\cdot 19\cdot 37\cdot 7\cdot 887 \\ 3^2\cdot 5\cdot 19\cdot 37\cdot 7103 \end{cases}$$

$$\text{XI. } \begin{cases} 3^4\cdot 5\cdot 11\cdot 29\cdot 89 \\ 3^4\cdot 5\cdot 11\cdot 2699 \end{cases} \qquad \text{XII. } \begin{cases} 3^2\cdot 7^2\cdot 11\cdot 13\cdot 41\cdot 461 \\ 3^2\cdot 7^2\cdot 11\cdot 13\cdot 19403 \end{cases}$$

$$\text{XIII. } \begin{cases} 3^2\cdot 5\cdot 13\cdot 19\cdot 29\cdot 569 \\ 3^2\cdot 5\cdot 13\cdot 19\cdot 17099 \end{cases} \qquad \text{XIV. } \begin{cases} 3^2\cdot 7^2\cdot 13\cdot 97\cdot 5\cdot 193 \\ 3^2\cdot 7^2\cdot 13\cdot 97\cdot 1163 \end{cases}$$

$$\text{XV. } \begin{cases} 3^2\cdot 7\cdot 13\cdot 41\cdot 163\cdot 5\cdot 977 \\ 3^2\cdot 7\cdot 13\cdot 41\cdot 163\cdot 5867 \end{cases} \qquad \text{XVI. } \begin{cases} 2^3\cdot 17\cdot 79 \\ 2^3\cdot 23\cdot 59 \end{cases}$$

XVII. $\begin{cases} 2^4 \cdot 23 \cdot 1367 \\ 2^4 \cdot 53 \cdot 607 \end{cases}$

XVIII. $\begin{cases} 2^4 \cdot 47 \cdot 89 \\ 2^4 \cdot 53 \cdot 79 \end{cases}$

XIX. $\begin{cases} 2^4 \cdot 23 \cdot 479 \\ 2^4 \cdot 89 \cdot 127 \end{cases}$

XX. $\begin{cases} 2^4 \cdot 23 \cdot 467 \\ 2^4 \cdot 103 \cdot 107 \end{cases}$

XXI. $\begin{cases} 2^4 \cdot 17 \cdot 5119 \\ 2^4 \cdot 239 \cdot 383 \end{cases}$

XXII. $\begin{cases} 2^4 \cdot 17 \cdot 10303 \\ 2^4 \cdot 167 \cdot 1103 \end{cases}$

XXIII. $\begin{cases} 2^4 \cdot 19 \cdot 1439 \\ 2^4 \cdot 149 \cdot 191 \end{cases}$

XXIV. $\begin{cases} 2^5 \cdot 59 \cdot 1103 \\ 2^5 \cdot 79 \cdot 827 \end{cases}$

XXV. $\begin{cases} 2^5 \cdot 37 \cdot 12671 \\ 2^5 \cdot 227 \cdot 2111 \end{cases}$

XXVI. $\begin{cases} 2^5 \cdot 53 \cdot 10559 \\ 2^5 \cdot 79 \cdot 7127 \end{cases}$

XXVII. $\begin{cases} 2^6 \cdot 79 \cdot 11087 \\ 2^6 \cdot 383 \cdot 2309 \end{cases}$

XXVIII. $\begin{cases} 2^8 \cdot 383 \cdot 9203 \\ 2^8 \cdot 1151 \cdot 3067 \end{cases}$

XXIX. $\begin{cases} 2^2 \cdot 11 \cdot 17 \cdot 263 \\ 2^2 \cdot 11 \cdot 43 \cdot 107 \end{cases}$

XXX. $\begin{cases} 3^3 \cdot 5 \cdot 7 \cdot 71 \\ 3^3 \cdot 5 \cdot 17 \cdot 31 \end{cases}$

XXXI. $\begin{cases} 3^2 \cdot 5 \cdot 13 \cdot 29 \cdot 79 \\ 3^2 \cdot 5 \cdot 13 \cdot 11 \cdot 199 \end{cases}$

XXXII. $\begin{cases} 3^2 \cdot 5 \cdot 13 \cdot 19 \cdot 47 \\ 3^2 \cdot 5 \cdot 13 \cdot 29 \cdot 31 \end{cases}$

XXXIII. $\begin{cases} 3^2 \cdot 5 \cdot 13 \cdot 19 \cdot 37 \cdot 1583 \\ 3^2 \cdot 5 \cdot 13 \cdot 19 \cdot 227 \cdot 263 \end{cases}$

XXXIV. $\begin{cases} 3^2 \cdot 7^2 \cdot 13 \cdot 19 \cdot 11 \cdot 220499 \\ 3^2 \cdot 7^2 \cdot 13 \cdot 19 \cdot 89 \cdot 29399 \end{cases}$ [1]

XXXV. $\begin{cases} 3^2 \cdot 5 \cdot 19 \cdot 37 \cdot 47 \\ 3^2 \cdot 5 \cdot 19 \cdot 7 \cdot 227 \end{cases}$

XXXVI. $\begin{cases} 2^4 \cdot 67 \cdot 37 \cdot 2411 \\ 2^4 \cdot 67 \cdot 227 \cdot 401 \end{cases}$

---

1) EULERUS numerum 220499 inter primos numeravit. At etiam si esset primus, tamen non essent amicabiles isti numeri. Esset quidem $\int 11 \cdot 220499 = 2646000 = \int 89 \cdot 29399$, at valores

$$\int 3^2 \cdot 7^2 \cdot 13 \cdot 19 \cdot \int 11 \cdot 220499 = 548992080000$$

et

$$3^2 \cdot 7^2 \cdot 13 \cdot 19 (11 \cdot 220499 + 89 \cdot 29399) = 549209934000$$

inter se discrepant (§ 22). Revera autem est $220499 = 311 \cdot 709$. Quamobrem hoc par XXXIV est delendum. F. R.

XXXVII. $\begin{cases} 3^2\cdot 5\cdot 7\cdot 11\cdot 29 \\ 3^2\cdot 5\cdot 31\cdot 89 \end{cases}$ [1])

XXXVIII. $\begin{cases} 2\cdot 5\cdot 23\cdot 29\cdot 673 \\ 2\cdot 5\cdot 7\cdot 60659 \end{cases}$

XXXIX. $\begin{cases} 2\cdot 5\cdot 7\cdot 19\cdot 107 \\ 2\cdot 5\cdot 47\cdot 359 \end{cases}$

XL. $\begin{cases} 2^3\cdot 11\cdot 163\cdot 191 \\ 2^3\cdot 31\cdot 11807 \end{cases}$

XLI. $\begin{cases} 3^2\cdot 7\cdot 13\cdot 23\cdot 11\cdot 19\cdot 367 \\ 3^2\cdot 7\cdot 13\cdot 23\cdot 79\cdot 1103 \end{cases}$

XLII. $\begin{cases} 3^3\cdot 5\cdot 23\cdot 11\cdot 19\cdot 367 \\ 3^3\cdot 5\cdot 23\cdot 79\cdot 1103 \end{cases}$

XLIII. $\begin{cases} 2^3\cdot 11\cdot 59\cdot 173 \\ 2^3\cdot 47\cdot 2609 \end{cases}$ [2])

XLIV. $\begin{cases} 2^3\cdot 11\cdot 23\cdot 2543 \\ 2^3\cdot 383\cdot 1907 \end{cases}$

XLV. $\begin{cases} 2^3\cdot 11\cdot 23\cdot 1871 \\ 2^3\cdot 467\cdot 1151 \end{cases}$

XLVI. $\begin{cases} 2^3\cdot 11\cdot 23\cdot 1619 \\ 2^3\cdot 647\cdot 719 \end{cases}$

XLVII. $\begin{cases} 2^3\cdot 11\cdot 29\cdot 239 \\ 2^3\cdot 191\cdot 449 \end{cases}$

XLVIII. $\begin{cases} 2^3\cdot 29\cdot 47\cdot 59 \\ 2^3\cdot 17\cdot 4799 \end{cases}$

XLIX. $\begin{cases} 2^4\cdot 17\cdot 167\cdot 13679 \\ 2^4\cdot 809\cdot 51071 \end{cases}$

L. $\begin{cases} 2^4\cdot 23\cdot 47\cdot 9767 \\ 2^4\cdot 1583\cdot 7103 \end{cases}$

LI. $\begin{cases} 2^2\cdot 5\cdot 13\cdot 1187 \\ 2^2\cdot 43\cdot 2267 \end{cases}$

LII. $\begin{cases} 3^2\cdot 7\cdot 13\cdot 5\cdot 17\cdot 1187 \\ 3^2\cdot 7\cdot 13\cdot 131\cdot 971 \end{cases}$

LIII. $\begin{cases} 3^5\cdot 7^2\cdot 13\cdot 53\cdot 11\cdot 211 \\ 3^5\cdot 7^2\cdot 13\cdot 53\cdot 2543 \end{cases}$

LIV. $\begin{cases} 3^2\cdot 5^2\cdot 11\cdot 59\cdot 179 \\ 3^2\cdot 5^2\cdot 17\cdot 19\cdot 359 \end{cases}$

LV. $\begin{cases} 3^3\cdot 5\cdot 17\cdot 23\cdot 397 \\ 3^3\cdot 5\cdot 7\cdot 21491 \end{cases}$

LVI. $\begin{cases} 3^4\cdot 7\cdot 11^2\cdot 19\cdot 47\cdot 7019 \\ 3^4\cdot 7\cdot 11^2\cdot 19\cdot 389\cdot 863 \end{cases}$

---

1) In editione principe (atque etiam in *Comment. arithm.*) legitur $3^3\cdot 5\cdot 7\cdot 11\cdot 29$ et $3^3\cdot 5\cdot 31\cdot 89$. Hi autem numeri non sunt amicabiles. Est quidem $\int 7\cdot 11\cdot 29 = 2880 = \int 31\cdot 89$, at valores $\int 3^3\cdot 5\cdot \int 7\cdot 11\cdot 29 = 691200$ et $3^3\cdot 5(7\cdot 11\cdot 29 + 31\cdot 89) = 673920$ inter se discrepant. Ex aequatione autem $z(7\cdot 11\cdot 29 + 31\cdot 89) = \int z\cdot\int 7\cdot 11\cdot 29$ seu

$$\frac{z}{\int z} = \frac{2880}{4992} = \frac{3\cdot 5}{2\cdot 13} = \frac{3\cdot 5}{2\cdot 13}\ \boxed{\frac{5}{6}}\ \frac{3^2}{13}\ \boxed{\frac{3^2}{13}}$$

invenitur $z = 3^2\cdot 5$. F. R.

2) In editione principe (atque etiam in *Comment. arithm.*) legitur *57* loco 47. Hoc autem par XLIII est idem atque par XXVIII tabulae p. 61. Falsum numerum 57 typographico tantum errore ortum esse manifestum est. F. R.

$$\text{LVII.} \begin{cases} 3^4 \cdot 7 \cdot 11^2 \cdot 19 \cdot 53 \cdot 6959 \\ 3^4 \cdot 7 \cdot 11^2 \cdot 19 \cdot 179 \cdot 2087 \end{cases} \qquad \text{LVIII.} \begin{cases} 3^5 \cdot 7^2 \cdot 13 \cdot 19 \cdot 47 \cdot 7019 \\ 3^5 \cdot 7^2 \cdot 13 \cdot 19 \cdot 389 \cdot 863 \end{cases}$$

$$\text{LIX.} \begin{cases} 3^5 \cdot 7^2 \cdot 13 \cdot 19 \cdot 53 \cdot 6959 \\ 3^5 \cdot 7^2 \cdot 13 \cdot 19 \cdot 179 \cdot 2087. \end{cases}$$

His adiicere lubet[1]) duo paria sequentia, quae sunt formae diversae a praecedentibus,

$$\text{LX.} \begin{cases} 2^3 \cdot 19 \cdot 41 \\ 2^5 \cdot 199 \end{cases} \qquad \text{LXI.} \begin{cases} 2^3 \cdot 41 \cdot 467 \\ 2^5 \cdot 19 \cdot 233. \end{cases}$$

---

1) Adiicere autem lubet etiam paria VIII et IX, quae inveniuntur in tabula p. 61 nec non in § 68, 78, 113 huius Commentationis. Redeunt enim ad haec duo illa quatuor, quorum mentionem facit P. H. Fuss in Prooemio *Comment. arithm.* (p. XXVI et LXXXI), quia par XIII illius tabulae non valet et par XXVIII congruit cum pari XLIII huius tabulae.

In summa igitur Eulerus tribus paribus numerorum amicabilium ante cognitis 59 nova adiecit, siquidem error nota 1 p. 161 correctus typographi esse existimandus sit. F. R.

OBSERVATIONES ANALYTICAE VARIAE DE COMBINATIONIBUS[1]

Commentatio 158 indicis ENESTROEMIANI
Commentarii academiae scientiarum Petropolitanae **13** (1741/3), 1751, p. 64—93

1. Proposita nobis sit series quantitatum quarumcunque sive finita sive in infinitum excurrens haec

$$a, \; b, \; c, \; d, \; e, \; f, \; g, \; h \text{ etc.},$$

quae litterae denotent quantitates quascunque sive inter se aequales sive inaequales. Interim tamen quantitates, quae diversis litteris indicantur, inter se inaequales vocabo, etiamsi in exemplis earum loco numeros aequales substituere liceat.

2. Nunc primo ex his quantitatibus formentur potestatibus sumendis novae series, quarum summae designentur litteris maiusculis A, B, C, D etc., ut sequitur; sit scilicet:

$$\begin{aligned} A &= a + b + c + d + e + \text{etc.}, \\ B &= a^2 + b^2 + c^2 + d^2 + e^2 + \text{etc.}, \\ C &= a^3 + b^3 + c^3 + d^3 + e^3 + \text{etc.}, \\ D &= a^4 + b^4 + c^4 + d^4 + e^4 + \text{etc.}, \\ E &= a^5 + b^5 + c^5 + d^5 + e^5 + \text{etc.} \\ &\text{etc.}, \end{aligned}$$

1) Vide etiam Commentationes 191 et 394 in hoc vol. 2 et in vol. 3 contentas nec non L. EULERI *Introductionem in analysin infinitorum*, Lausannae 1748, t. I cap. XVI; *LEONHARDI EULERI Opera omnia*, series I, vol. 8. F. R.

quae series singulae erunt infinitae, si numerus quantitatum a, b, c, d etc. assumtarum fuerit infinitus; sin autem numerus harum quantitatum sit finitus ac determinatus, puta $= n$, tum singulae istae series totidem terminos complectentur.

3. Deinde sequenti modo ex quantitatibus assumtis a, b, c, d etc. productis inaequalium sumendis formentur series. Primo scilicet colligantur quantitates singulae, tum facta ex binis inaequalibus, tertio ex ternis inaequalibus, quarto ex quaternis inaequalibus, et ita porro; atque hae series litteris graecis α, β, γ, δ etc. indicentur, ut sequitur:

$$\alpha = a + b + c + d + \text{etc.},$$
$$\beta = ab + ac + ad + ae + bd + \text{etc.},$$
$$\gamma = abc + abd + abe + bcd + \text{etc.},$$
$$\delta = abcd + abce + bcde + \text{etc.},$$
$$\varepsilon = abcde + \text{etc.}$$
$$\text{etc.};$$

quae series, si quantitatum assumtarum a, b, c, d etc. numerus fuerit infinitus, non solum omnes in infinitum excurrent, sed etiam ipsarum serierum hoc modo formandarum numerus erit infinitus. Quodsi autem numerus quantitatum a, b, c, d etc. fuerit finitus, puta $= n$, tum series α continebit n terminos, secunda series β constabit ex $\frac{n(n-1)}{1\cdot 2}$ terminis, tertia γ ex $\frac{n(n-1)(n-2)}{1\cdot 2\cdot 3}$ terminis, quarta δ ex $\frac{n(n-1)(n-2)(n-3)}{1\cdot 2\cdot 3\cdot 4}$ terminis, et ita porro, donec tandem ad seriem perveniatur ex unico termino constantem, quam sequentes omnes evanescent terminis omnino carentes. Perspicuum autem est serierum, quae hoc modo generantur, numerum fore $= n$ earumque ultimam unico constare termino, qui sit productum ex omnibus quantitatibus assumtis a, b, c, d, e etc.

4. Quemadmodum autem hic producta ex quantitatibus inaequalibus tantum assumsimus ex iisque series expositas formavimus, ita iisdem quantitatibus in productis, quoties fieri poterit, repetendis nanciscemur novas productorum ex singulis, binis, ternis, quaternis etc. series, in quibus factores aequales non ut ante excludantur; hae ergo series ita se habebunt:

$$\mathfrak{A} = a + b + c + d + e + \text{etc.},$$

$$\mathfrak{B} = a^2 + ab + b^2 + ac + bc + c^2 + \text{etc.},$$

$$\mathfrak{C} = a^3 + a^2b + ab^2 + b^3 + a^2c + abc + \text{etc.},$$

$$\mathfrak{D} = a^4 + a^3b + a^2b^2 + a^2bc + abcd + \text{etc.},$$

$$\mathfrak{E} = a^5 + a^4b + a^3b^2 + a^3bc + a^2bcd + \text{etc.}$$

etc.;

in his nempe seriebus omnes continentur quantitates, quae per multiplicationem ex quantitatibus assumtis a, b, c, d etc. produci possunt. Ceterum notandum est, si numerus quantitatum a, b, c, d etc. fuerit finitus $= n$, tum seriem primam $\mathfrak{A}$ esse habituram n terminos; secunda autem $\mathfrak{B}$ habebit $\frac{n(n+1)}{1\cdot 2}$ terminos, tertia $\mathfrak{C}$ habebit $\frac{n(n+1)(n+2)}{1\cdot 2\cdot 3}$ terminos, quarta $\mathfrak{D}$ vero $\frac{n(n+1)(n+2)(n+3)}{1\cdot 2\cdot 3\cdot 4}$ terminos, et ita porro.

5. Tres hi serierum, quas ex quantitatibus assumtis a, b, c, d etc. triplici modo composuimus, ordines multifariam inter se connectuntur, ita ut uno serierum ordine cognito bini reliqui ordines inde possint determinari. Atque in hoc negotio ad connexionis legem et rationem investigandam observatio atque inductio plurimum adhiberi solet; hocque pacto primum quidem certissime constat esse $A = \alpha = \mathfrak{A}$ ac de reliquis compertum est esse

$$\alpha = A,$$

$$\beta = \frac{\alpha A - B}{2},$$

$$\gamma = \frac{\beta A - \alpha B + C}{3},$$

$$\delta = \frac{\gamma A - \beta B + \alpha C - D}{4},$$

$$\varepsilon = \frac{\delta A - \gamma B + \beta C - \alpha D + E}{5}$$

etc.

item

$$\mathfrak{A} = A,$$

$$\mathfrak{B} = \frac{\mathfrak{A}A + B}{2},$$

$$\mathfrak{C} = \frac{\mathfrak{B}A + \mathfrak{A}B + C}{3},$$

$$\mathfrak{D} = \frac{\mathfrak{C}A + \mathfrak{B}B + \mathfrak{A}C + D}{4},$$

$$\mathfrak{E} = \frac{\mathfrak{D}A + \mathfrak{C}B + \mathfrak{B}C + \mathfrak{A}D + E}{5}$$

etc.

praetereaque

$$\mathfrak{A} = \alpha,$$

$$\mathfrak{B} = \alpha\mathfrak{A} - \beta,$$

$$\mathfrak{C} = \alpha\mathfrak{B} - \beta\mathfrak{A} + \gamma,$$

$$\mathfrak{D} = \alpha\mathfrak{C} - \beta\mathfrak{B} + \gamma\mathfrak{A} - \delta,$$

$$\mathfrak{E} = \alpha\mathfrak{D} - \beta\mathfrak{C} + \gamma\mathfrak{B} - \delta\mathfrak{A} + \varepsilon$$

etc.

Harumque relationum ope ex datis summis serierum cuiuscunque classis definiri poterunt summae serierum, quae in duabus reliquis classibus continentur.

6. Ad naturam atque indolem harum serierum diligentius attendenti facile quidem per observationem et inductionem veritas istius mutuae relationis patebit. Verum tamen quo magis de veritate huius nexus convincamur, expediet sequenti modo totum hoc negotium considerare; quo simul aliae insuper proprietates nobis offerentur, ad quas sola inductio non tam facile viam aperit. Assumtis scilicet pro libitu quantitatibus

$$a,\ b,\ c,\ d,\ e \text{ etc.}$$

ex iisque formatis trium classium seriebus supra memoratis contemplemur hanc expressionem

$$P = \frac{az}{1-az} + \frac{bz}{1-bz} + \frac{cz}{1-cz} + \frac{dz}{1-dz} + \frac{ez}{1-ez} + \text{etc.},$$

cuius singuli termini in progressiones geometricas resoluti more solito dabunt

$$\begin{aligned} P = &+ z\,(a + b + c + d + e + \text{etc.}) \\ &+ z^2(a^2 + b^2 + c^2 + d^2 + e^2 + \text{etc.}) \\ &+ z^3(a^3 + b^3 + c^3 + d^3 + e^3 + \text{etc.}) \\ &+ z^4(a^4 + b^4 + c^4 + d^4 + e^4 + \text{etc.}) \\ &\quad \text{etc.}, \end{aligned}$$

quae series omnes in prima classe continentur. Quare si earum loco summae supra (§ 2) positae scribantur, fiet

$$P = Az + Bz^2 + Cz^3 + Dz^4 + Ez^5 + \text{etc.},$$

cuius idcirco seriei summa erit, uti sumsimus,

$$P = \frac{az}{1 - az} + \frac{bz}{1 - bz} + \frac{cz}{1 - cz} + \frac{dz}{1 - dz} + \text{etc.}$$

Simili autem modo si fuerit

$$Q = \frac{az}{1 + az} + \frac{bz}{1 + bz} + \frac{cz}{1 + cz} + \frac{dz}{1 + dz} + \text{etc.},$$

erit per series primae classis

$$Q = Az - Bz^2 + Cz^3 - Dz^4 + Ez^5 - \text{etc.}$$

7. Consideremus porro hanc expressionem

$$R = (1 + az)(1 + bz)(1 + cz)(1 + dz)(1 + ez) \text{ etc.};$$

cuius factores si actu in se multiplicentur ac termini secundum exponentes ipsius z disponantur, fiet coefficiens ipsius z aequalis summae quantitatum assumtarum a, b, c, d etc. Coefficiens ipsius z^2 erit aggregatum omnium productorum ex binis inaequalibus, coefficiens ipsius z^3 erit aggregatum omnium productorum ex ternis inaequalibus, et ita porro; ex quibus sequitur fore

$$R = 1 + \alpha z + \beta z^2 + \gamma z^3 + \delta z^4 + \varepsilon z^5 + \text{etc.}$$

secundum definitiones supra (§ 3) datas.

Quodsi autem ponatur

$$S = (1 - az)(1 - bz)(1 - cz)(1 - dz)(1 - ez) \text{ etc.},$$

erit faciendo tantum z negativo

$$S = 1 - \alpha z + \beta z^2 - \gamma z^3 + \delta z^4 - \varepsilon z^5 + \text{etc.}$$

8. Ut series hae R et S cum praecedentibus P et Q comparentur, notandum est esse

$$lR = l(1 + az) + l(1 + bz) + l(1 + cz) + l(1 + dz) + \text{etc.},$$

unde sumendis differentialibus erit

$$\frac{dR}{Rdz} = \frac{a}{1 + az} + \frac{b}{1 + bz} + \frac{c}{1 + cz} + \frac{d}{1 + dz} + \text{etc.},$$

quae per z multiplicata dat illam ipsam expressionem, quam supra Q vocavimus, ita ut sit

$$Q = \frac{zdR}{Rdz}.$$

Simili autem modo erit

$$\frac{dS}{Sdz} = -\frac{a}{1 - az} - \frac{b}{1 - bz} - \frac{c}{1 - cz} - \text{etc.},$$

unde habebitur

$$P = \frac{-zdS}{Sdz}.$$

9. Cum nunc sit

$$R = 1 + \alpha z + \beta z^2 + \gamma z^3 + \text{etc.},$$

erit

$$\frac{zdR}{dz} = \alpha z + 2\beta z^2 + 3\gamma z^3 + 4\delta z^4 + 5\varepsilon z^5 + \text{etc.}$$

ideoque

$$Q = Az - Bz^2 + Cz^3 - Dz^4 + Ez^5 - \text{etc.}$$

$$= \frac{\alpha z + 2\beta z^2 + 3\gamma z^3 + 4\delta z^4 + 5\varepsilon z^5 + \text{etc.}}{1 + \alpha z + \beta z^2 + \gamma z^3 + \delta z^4 + \varepsilon z^5 + \text{etc.}}.$$

At ex aequalitate harum expressionum sequuntur sequentes relationes inter litteras A, B, C, D etc. et α, β, γ, δ, ε etc.

$$\begin{aligned}
&A = \alpha,\\
&\alpha A - B = 2\beta,\\
&\beta A - \alpha B + C = 3\gamma,\\
&\gamma A - \beta B + \alpha C - D = 4\delta,\\
&\delta A - \gamma B + \beta C - \alpha D + E = 5\varepsilon\\
&\qquad\qquad \text{etc.}
\end{aligned}$$

Simili vero modo ex altera aequatione $P = \frac{-z\,dS}{S\,dz}$ sequitur

$$P = Az + Bz^2 + Cz^3 + Dz^4 + Ez^5 + \text{etc.}$$
$$= \frac{\alpha z - 2\beta z^2 + 3\gamma z^3 - 4\delta z^4 + 5\varepsilon z^5 - \text{etc.}}{1 - \alpha z + \beta z^2 - \gamma z^3 + \delta z^4 - \varepsilon z^5 + \text{etc.}},$$

quae pariter easdem praebet determinationes, quas supra (§ 5) tradidimus.

10. Praeterea autem ex aequatione $Q = \frac{z\,dR}{R\,dz}$ consequimur integrando $\int \frac{Q\,dz}{z} = lR$. Quoniam vero est $Q = Az - Bz^2 + Cz^3 - Dz^4 + \text{etc.}$, erit

$$\int \frac{Q\,dz}{z} = Az - \frac{Bz^2}{2} + \frac{Cz^3}{3} - \frac{Dz^4}{4} + \text{etc.},$$

cuius seriei valor itaque exprimet logarithmum huius seriei

$$R = 1 + \alpha z + \beta z^2 + \gamma z^3 + \delta z^4 + \text{etc.}$$

Quemadmodum igitur est

$$l(1 + \alpha z + \beta z^2 + \gamma z^3 + \text{etc.}) = Az - \frac{1}{2}Bz^2 + \frac{1}{3}Cz^3 - \frac{1}{4}Dz^4 + \text{etc.},$$

ita etiam ex aequatione $\int \frac{P\,dz}{z} = -lS$ erit

$$l(1 - \alpha z + \beta z^2 - \gamma z^3 + \text{etc.}) = -Az - \frac{1}{2}Bz^2 - \frac{1}{3}Cz^3 - \frac{1}{4}Dz^4 - \text{etc.}$$

Quare si k scribatur pro numero, cuius logarithmus hyperbolicus est $=1$, habebitur

$$1+\alpha z+\beta z^2+\gamma z^3+\delta z^4+\text{etc.}=k^{Az-\frac{1}{2}Bz^2+\frac{1}{3}Cz^3-\frac{1}{4}Dz^4+\text{etc}}$$

et

$$1-\alpha z+\beta z^2-\gamma z^3+\delta z^4-\text{etc.}=k^{-Az-\frac{1}{2}Bz^2-\frac{1}{3}Cz^3-\frac{1}{4}Dz^4-\text{etc}}.$$

11. Notatu praeterea dignae sunt expressiones harum R et S reciprocae, nempe $\frac{1}{R}$ et $\frac{1}{S}$. Est vero

$$\frac{1}{S}=\frac{1}{(1-az)(1-bz)(1-cz)(1-dz)\text{ etc.}};$$

ad cuius fractionis valorem per seriem, cuius termini secundum potestates ipsius z progrediantur, exprimendum, perspicuum est in se invicem multiplicari oportere cunctas has progressiones geometricas

$$\frac{1}{1-az}=1+az+a^2z^2+a^3z^3+a^4z^4+\text{etc.},$$

$$\frac{1}{1-bz}=1+bz+b^2z^2+b^3z^3+b^4z^4+\text{etc.},$$

$$\frac{1}{1-cz}=1+cz+c^2z^2+c^3z^3+c^4z^4+\text{etc.},$$

$$\frac{1}{1-dz}=1+dz+d^2z^2+d^3z^3+d^4z^4+\text{etc.}$$

etc.

In producto autem post primum terminum 1 coefficiens ipsius z erit summa quantitatum $a+b+c+d+$ etc., coefficiens ipsius z^2 erit summa factorum ex binis non excipiendo factores aequales in eodem facto, coefficiens ipsius z^3 erit summa factorum ex ternis, et ita porro, quas productorum summas supra (§ 4) litteris alphabeti germanici $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, $\mathfrak{E}$ etc. designavimus. His itaque litteris introductis habebimus

$$\frac{1}{S}=1+\mathfrak{A}z+\mathfrak{B}z^2+\mathfrak{C}z^3+\mathfrak{D}z^4+\mathfrak{E}z^5+\text{etc.}$$

atque simili modo valorem ipsius R tractando erit

$$\frac{1}{R}=1-\mathfrak{A}z+\mathfrak{B}z^2-\mathfrak{C}z^3+\mathfrak{D}z^4-\mathfrak{E}z^5+\text{etc.}$$

12. Hae ergo series reciprocae sunt earum, quas supra sub litteris R et S (§ 7) protulimus. Atque hanc ob causam erit

$$1 = (1 + \alpha z + \beta z^2 + \gamma z^3 + \delta z^4 + \text{etc.})(1 - \mathfrak{A} z + \mathfrak{B} z^2 - \mathfrak{C} z^3 + \mathfrak{D} z^4 + \text{etc.})$$

pariterque

$$1 = (1 - \alpha z + \beta z^2 - \gamma z^3 + \delta z^4 - \text{etc.})(1 + \mathfrak{A} z + \mathfrak{B} z^2 + \mathfrak{C} z^3 + \mathfrak{D} z^4 + \text{etc.}).$$

Ex utraque autem sequitur una eademque relatio inter valores litterarum $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ etc. et α, β, γ, δ etc.; erit scilicet

$$\begin{gathered}\mathfrak{A} - \alpha = 0,\\ \mathfrak{B} - \alpha\mathfrak{A} + \beta = 0,\\ \mathfrak{C} - \alpha\mathfrak{B} + \beta\mathfrak{A} - \gamma = 0,\\ \mathfrak{D} - \alpha\mathfrak{C} + \beta\mathfrak{B} - \gamma\mathfrak{A} + \delta = 0\\ \text{etc.},\end{gathered}$$

quam eandem relationem iam supra (§ 5) tradidimus.

13. Quodsi ponamus $\frac{1}{R} = T$ et $\frac{1}{S} = V$, ut sit

$$T = 1 - \mathfrak{A} z + \mathfrak{B} z^2 - \mathfrak{C} z^3 + \mathfrak{D} z^4 - \text{etc.}$$

et

$$V = 1 + \mathfrak{A} z + \mathfrak{B} z^2 + \mathfrak{C} z^3 + \mathfrak{D} z^4 + \text{etc.},$$

erit

$$\frac{dR}{R} = -\frac{dT}{T} \quad \text{et} \quad \frac{dS}{S} = -\frac{dV}{V}$$

hincque fiet

$$P = \frac{z\,dV}{V\,dz} \quad \text{et} \quad Q = -\frac{z\,dT}{T\,dz}.$$

Quare cum sit

$$\frac{z\,dV}{dz} = \mathfrak{A} z + 2\mathfrak{B} z^2 + 3\mathfrak{C} z^3 + 4\mathfrak{D} z^4 + \text{etc.}$$

et

$$-\frac{z\,dT}{dz} = \mathfrak{A} z - 2\mathfrak{B} z^2 + 3\mathfrak{C} z^3 - 4\mathfrak{D} z^4 + \text{etc.},$$

habebimus loco P et Q valores debitos ex § 6 scribendo has aequationes

$$Az + Bz^2 + Cz^3 + Dz^4 + \text{etc.} = \frac{\mathfrak{A}z + 2\mathfrak{B}z^2 + 3\mathfrak{C}z^3 + 4\mathfrak{D}z^4 + \text{etc.}}{1 + \mathfrak{A}z + \mathfrak{B}z^2 + \mathfrak{C}z^3 + \mathfrak{D}z^4 + \text{etc.}}$$

et

$$Az - Bz^2 + Cz^3 - Dz^4 + \text{etc.} = \frac{\mathfrak{A}z - 2\mathfrak{B}z^2 + 3\mathfrak{C}z^3 - 4\mathfrak{D}z^4 + \text{etc.}}{1 - \mathfrak{A}z + \mathfrak{B}z^2 - \mathfrak{C}z^3 + \mathfrak{D}z^4 - \text{etc.}},$$

ex quibus eadem sequitur relatio inter litteras A, B, C, D etc. et $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ etc., quam supra (§ 5) dedimus. Erit scilicet

$$\mathfrak{A} = A,$$
$$2\mathfrak{B} = \mathfrak{A}A + B,$$
$$3\mathfrak{C} = \mathfrak{B}A + \mathfrak{A}B + C,$$
$$4\mathfrak{D} = \mathfrak{C}A + \mathfrak{B}B + \mathfrak{A}C + D,$$
$$5\mathfrak{E} = \mathfrak{D}A + \mathfrak{C}B + \mathfrak{B}C + \mathfrak{A}D + E$$
$$\text{etc.}$$

14. Ex aequationibus § 12 datis sequitur fore

$$l(1 + \alpha z + \beta z^2 + \gamma z^3 + \text{etc.}) = -l(1 - \mathfrak{A}z + \mathfrak{B}z^2 - \mathfrak{C}z^3 + \text{etc.})$$

et

$$l(1 - \alpha z + \beta z^2 - \gamma z^3 + \text{etc.}) = -l(1 + \mathfrak{A}z + \mathfrak{B}z^2 + \mathfrak{C}z^3 + \text{etc.}).$$

His igitur ad § 10 accommodatis erit

$$l(1 - \mathfrak{A}z + \mathfrak{B}z^2 - \mathfrak{C}z^3 + \text{etc.}) = -Az + \frac{1}{2}Bz^2 - \frac{1}{3}Cz^3 + \frac{1}{4}Dz^4 - \text{etc.}$$

et

$$l(1 + \mathfrak{A}z + \mathfrak{B}z^2 + \mathfrak{C}z^3 + \text{etc.}) = Az + \frac{1}{2}Bz^2 + \frac{1}{3}Cz^3 + \frac{1}{4}Dz^4 + \text{etc.}$$

Hincque sumto k pro numero, cuius logarithmus $= 1$, erit

$$1 - \mathfrak{A}z + \mathfrak{B}z^2 - \mathfrak{C}z^3 + \text{etc.} = k^{-Az + \frac{1}{2}Bz^2 - \frac{1}{3}Cz^3 + \frac{1}{4}Dz^4 - \text{etc.}}$$

atque

$$1 + \mathfrak{A}z + \mathfrak{B}z^2 + \mathfrak{C}z^3 + \text{etc.} = k^{Az + \frac{1}{2}Bz^2 + \frac{1}{3}Cz^3 + \frac{1}{4}Dz^4 + \text{etc.}}.$$

15. Si iam litterae R et S retineant valores supra assumtos (§ 7), erit

$$1 + \alpha z + \beta z^2 + \gamma z^3 + \delta z^4 + \text{etc.} = R,$$

$$1 - \mathfrak{A} z + \mathfrak{B} z^2 - \mathfrak{C} z^3 + \mathfrak{D} z^4 - \text{etc.} = \frac{1}{R}$$

et

$$1 - \alpha z + \beta z^2 - \gamma z^3 + \delta z^4 - \text{etc.} = S,$$

$$1 + \mathfrak{A} z + \mathfrak{B} z^2 + \mathfrak{C} z^3 + \mathfrak{D} z^4 + \text{etc.} = \frac{1}{S}.$$

Ex quibus deducuntur sequentia consectaria

$$1 + \beta z^2 + \delta z^4 + \zeta z^6 + \theta z^8 + \text{etc.} = \frac{R+S}{2},$$

$$\alpha z + \gamma z^3 + \varepsilon z^5 + \eta z^7 + \iota z^9 + \text{etc.} = \frac{R-S}{2},$$

$$1 + \mathfrak{B} z^2 + \mathfrak{D} z^4 + \mathfrak{F} z^6 + \mathfrak{H} z^8 + \text{etc.} = \frac{R+S}{2RS},$$

$$\mathfrak{A} z + \mathfrak{C} z^3 + \mathfrak{E} z^5 + \mathfrak{G} z^7 + \mathfrak{J} z^9 + \text{etc.} = \frac{R-S}{2RS}$$

hincque colligitur ista proportio

$$1 + \beta z^2 + \delta z^4 + \zeta z^6 + \text{etc.} : \alpha z + \gamma z^3 + \varepsilon z^5 + \eta z^7 + \text{etc.}$$
$$= 1 + \mathfrak{B} z^2 + \mathfrak{D} z^4 + \mathfrak{F} z^6 + \text{etc.} : \mathfrak{A} z + \mathfrak{C} z^3 + \mathfrak{E} z^5 + \mathfrak{G} z^7 + \text{etc.}$$

Cum praeterea sit

$$R - 1 = \alpha z + \beta z^2 + \gamma z^3 + \delta z^4 + \text{etc.},$$

$$1 - \frac{1}{R} = \mathfrak{A} z - \mathfrak{B} z^2 + \mathfrak{C} z^3 - \mathfrak{D} z^4 + \text{etc.},$$

erit

$$R = \frac{\alpha z + \beta z^2 + \gamma z^3 + \delta z^4 + \text{etc.}}{\mathfrak{A} z - \mathfrak{B} z^2 + \mathfrak{C} z^3 - \mathfrak{D} z^4 + \text{etc.}}$$

similique modo propter

$$1 - S = \alpha z - \beta z^2 + \gamma z^3 - \delta z^4 + \text{etc.},$$

$$\frac{1}{S} - 1 = \mathfrak{A} z + \mathfrak{B} z^2 + \mathfrak{C} z^3 + \mathfrak{D} z^4 + \text{etc.}$$

erit

$$S = \frac{\alpha z - \beta z^2 + \gamma z^3 - \delta z^4 + \text{etc.}}{\mathfrak{A} z + \mathfrak{B} z^2 + \mathfrak{C} z^3 + \mathfrak{D} z^4 + \text{etc.}}.$$

16. Deinde vero si ut supra (§ 6) ponamus

$$P = Az + Bz^2 + Cz^3 + Dz^4 + \text{etc.},$$
$$Q = Az - Bz^2 + Cz^3 - Dz^4 + \text{etc.},$$

erit ex paragrapho 9

$$\alpha z + 2\beta z^2 + 3\gamma z^3 + 4\delta z^4 + \text{etc.} = QR,$$
$$\alpha z - 2\beta z^2 + 3\gamma z^3 - 4\delta z^4 + \text{etc.} = PS$$

similique modo ex paragrapho 13 habebitur

$$\mathfrak{A}z + 2\mathfrak{B}z^2 + 3\mathfrak{C}z^3 + 4\mathfrak{D}z^4 + \text{etc.} = \frac{P}{S},$$
$$\mathfrak{A}z - 2\mathfrak{B}z^2 + 3\mathfrak{C}z^3 + 4\mathfrak{D}z^4 + \text{etc.} = \frac{Q}{R}.$$

Ex quibus sequentia corollaria facile derivantur:

$$\frac{\alpha z - 2\beta z^2 + 3\gamma z^3 - 4\delta z^4 + \text{etc.}}{Az + Bz^2 + Cz^3 + Dz^4 + \text{etc.}} = S = \frac{Az + Bz^2 + Cz^3 + Dz^4 + \text{etc.}}{\mathfrak{A}z + 2\mathfrak{B}z^2 + 3\mathfrak{C}z^3 + 4\mathfrak{D}z^4 + \text{etc.}},$$
$$\frac{\alpha z + 2\beta z^2 + 3\gamma z^3 + 4\delta z^4 + \text{etc.}}{Az - Bz^2 + Cz^3 - Dz^4 + \text{etc.}} = R = \frac{Az - Bz^2 + Cz^3 - Dz^4 + \text{etc.}}{\mathfrak{A}z - 2\mathfrak{B}z^2 + 3\mathfrak{C}z^3 - 4\mathfrak{D}z^4 + \text{etc.}}.$$

Pro litteris igitur R et S habemus quintuplices valores hos

$$R = 1 + \alpha z + \beta z^2 + \gamma z^3 + \delta z^4 + \text{etc.},$$
$$R = \frac{1}{1 - \mathfrak{A}z + \mathfrak{B}z^2 - \mathfrak{C}z^3 + \mathfrak{D}z^4 - \text{etc.}},$$
$$R = \frac{\alpha z + \beta z^2 + \gamma z^3 + \delta z^4 + \text{etc.}}{\mathfrak{A}z - \mathfrak{B}z^2 + \mathfrak{C}z^3 - \mathfrak{D}z^4 + \text{etc.}},$$
$$R = \frac{\alpha z + 2\beta z^2 + 3\gamma z^3 + 4\delta z^4 + \text{etc.}}{Az - Bz^2 + Cz^3 - Dz^4 + \text{etc.}},$$
$$R = \frac{Az - Bz^2 + Cz^3 - Dz^4 + \text{etc.}}{\mathfrak{A}z - 2\mathfrak{B}z^2 + 3\mathfrak{C}z^3 - 4\mathfrak{D}z^4 + \text{etc.}},$$

qui posito $-z$ loco z totidem praebent valores pro S. Atque ex horum quinque valorum multiplici combinatione quam plurimae proprietates elici possunt, quas terni litterarum nostrarum ordines, scilicet $\alpha, \beta, \gamma, \delta$ etc., $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ etc., A, B, C, D etc., inter se tenent, quibus autem evolvendis hic supersedemus.

17. His, quae latissime patent, praemissis atque expositis ad magis particularia descendamus ac primo quidem pro serie litterarum a, b, c, d etc. accipiatur progressio geometrica infinita haec

$$n,\ n^2,\ n^3,\ n^4,\ n^5,\ n^6 \text{ etc.};$$

qua in formulas superiores successive introducta habebimus:

$$A = n + n^2 + n^3 + n^4 + n^5 + \text{etc.} = \frac{n}{1-n},$$

$$B = n^2 + n^4 + n^6 + n^8 + n^{10} + \text{etc.} = \frac{nn}{1-nn},$$

$$C = n^3 + n^6 + n^9 + n^{12} + n^{15} + \text{etc.} = \frac{n^3}{1-n^3},$$

$$D = n^4 + n^8 + n^{12} + n^{16} + n^{20} + \text{etc.} = \frac{n^4}{1-n^4}$$

etc.

Iam ex § 6 duplices pro litteris P et Q nanciscimur valores, qui erunt

$$P = \frac{nz}{1-nz} + \frac{n^2z}{1-n^2z} + \frac{n^3z}{1-n^3z} + \frac{n^4z}{1-n^4z} + \text{etc.},$$

$$Q = \frac{nz}{1+nz} + \frac{n^2z}{1+n^2z} + \frac{n^3z}{1+n^3z} + \frac{n^4z}{1+n^4z} + \text{etc.}$$

hincque ex inventis litterarum A, B, C, D etc. valoribus nascentur hi alteri

$$P = \frac{nz}{1-n} + \frac{n^2z^2}{1-nn} + \frac{n^3z^3}{1-n^3} + \frac{n^4z^4}{1-n^4} + \text{etc.},$$

$$Q = \frac{nz}{1-n} - \frac{n^2z^2}{1-nn} + \frac{n^3z^3}{1-n^3} - \frac{n^4z^4}{1-n^4} + \text{etc.}$$

18. Ex paragrapho porro 7 habebimus pro R et S sequentes expressiones

$$R = (1+nz)(1+n^2z)(1+n^3z)(1+n^4z) \text{ etc.},$$

$$S = (1-nz)(1-n^2z)(1-n^3z)(1-n^4z) \text{ etc.},$$

qui factores actu in se multiplicati et producta secundum dimensiones ipsius z ordinata praebebunt pro R et S has series

$$R = 1 + \alpha z + \beta z^2 + \gamma z^3 + \delta z^4 + \text{etc.},$$

$$S = 1 - \alpha z + \beta z^2 - \gamma z^3 + \delta z^4 - \text{etc.},$$

ubi litterae α, β, γ, δ etc. ex serie assumta n, n^2, n^3, n^4, n^5, n^6, n^7 etc. ita determinabuntur, ut sit:

I. $\alpha =$ summae singulorum terminorum; unde erit

$$\alpha = n + n^2 + n^3 + n^4 + n^5 + n^6 + n^7 + \text{etc.},$$

quae est ipsa progressio geometrica assumta, in qua quaevis potestas ipsius n occurrit atque coefficientem habet $+1$.

II. $\beta =$ summae factorum ex binis terminis; unde erit

$$\beta = n^3 + n^4 + 2n^5 + 2n^6 + 3n^7 + 3n^8 + 4n^9 + 4n^{10} + \text{etc.},$$

in qua serie post potestatem tertiam omnes sequentes ipsius n potestates occurrunt; quaelibet autem potestas toties occurrit, quoties ex multiplicatione binorum terminorum seriei α oriri potest. Cum autem multiplicatio potestatum consistat in exponentium additione, coefficiens cuiusque potestatis ipsius n in serie β ostendet, quot variis modis exponens ipsius n possit in duas partes inaequales distribui seu quoties iste exponens ex additione duorum numerorum integrorum inaequalium produci queat. Sic potestatis decimae n^{10} coefficiens est 4, quia 10 quatuor modis in duas partes inaequales distribui potest, nempe

$$10 = 1 + 9, \quad 10 = 3 + 7,$$
$$10 = 2 + 8, \quad 10 = 4 + 6.$$

III. $\gamma =$ summae factorum ex ternis terminis seriei α inaequalibus; unde erit

$$\gamma = n^6 + n^7 + 2n^8 + 3n^9 + 4n^{10} + 5n^{11} + 7n^{12} + 8n^{13} + \text{etc.},$$

in qua post potestatem sextam omnes sequentes ipsius n potestates occurrunt. Cuiuslibet autem potestatis coefficiens indicat, quot variis modis exponens distribui possit in tres partes inaequales seu quoties idem exponens produci queat ex additione trium numerorum integrorum inter se inaequalium. Sic potestas n^{12} coefficientem habet 7, quia exponens 12 septem modis in tres partes inaequales partiri potest, uti

$$12 = 1 + 2 + 9, \quad 12 = 1 + 5 + 6,$$
$$12 = 1 + 3 + 8, \quad 12 = 2 + 3 + 7,$$
$$12 = 1 + 4 + 7, \quad 12 = 2 + 4 + 6,$$
$$12 = 3 + 4 + 5.$$

IV. $\delta =$ summae factorum ex quatuor terminis seriei α inaequalibus inter se; unde erit

$$\delta = n^{10} + n^{11} + 2n^{12} + 3n^{13} + 5n^{14} + 6n^{15} + 9n^{16} + \text{etc.},$$

cuius prima potestas est n^{10}, quippe cuius exponens est $1 + 2 + 3 + 4$ seu numerus trigonalis quartus. Sequentium potestatum quaelibet toties adest, quoties eius exponens oriri potest ex additione quatuor numerorum integrorum inter se inaequalium. Sic potestas sexta decima n^{16} coefficientem habet 9, quia 16 novem modis in quatuor partes inter se inaequales dispertiri potest, quae novem partitiones sunt

$$16 = 1 + 2 + 3 + 10, \quad 16 = 1 + 3 + 4 + 8,$$
$$16 = 1 + 2 + 4 + 9, \quad 16 = 1 + 3 + 5 + 7,$$
$$16 = 1 + 2 + 5 + 8, \quad 16 = 1 + 4 + 5 + 6,$$
$$16 = 1 + 2 + 6 + 7, \quad 16 = 2 + 3 + 4 + 7,$$
$$16 = 2 + 3 + 5 + 6.$$

Simili modo res se habet in sequentium litterarum ε, ζ, η etc. valoribus, qui erunt

$$\varepsilon = n^{15} + n^{16} + 2n^{17} + 3n^{18} + 5n^{19} + 7n^{20} + 10n^{21} + \text{etc.},$$
$$\zeta = n^{21} + n^{22} + 2n^{23} + 3n^{24} + 5n^{25} + 7n^{26} + 11n^{27} + \text{etc.},$$
$$\eta = n^{28} + n^{29} + 2n^{30} + 3n^{31} + 5n^{32} + 7n^{33} + 11n^{34} + \text{etc.}$$
$$\text{etc.},$$

in quibus seriebus omnibus cuiusvis ipsius n potestatis coefficiens indicat, quot variis modis exponens ipsius n possit resolvi in tot partes inaequales, quota series est a principio numerata. Seu coefficiens cuiusque termini declarat, quoties exponens ipsius n oriri queat ex additione tot numerorum integrorum inter se inaequalium, quota ipsa series, ex qua terminus desumitur,

est numerando a prima α. Sic in serie septima coefficiens potestatis n^{34} est 11, quia numerus 34 undecim modis distribui potest in septem partes inaequales, quae distributiones sunt

$$34 = 1 + 2 + 3 + 4 + 5 + 6 + 13,$$
$$34 = 1 + 2 + 3 + 4 + 5 + 7 + 12,$$
$$34 = 1 + 2 + 3 + 4 + 5 + 8 + 11,$$
$$34 = 1 + 2 + 3 + 4 + 5 + 9 + 10,$$
$$34 = 1 + 2 + 3 + 4 + 6 + 7 + 11,$$
$$34 = 1 + 2 + 3 + 4 + 6 + 8 + 10,$$
$$34 = 1 + 2 + 3 + 4 + 7 + 8 + 9,$$
$$34 = 1 + 2 + 3 + 5 + 6 + 7 + 10,$$
$$34 = 1 + 2 + 3 + 5 + 6 + 8 + 9,$$
$$34 = 1 + 2 + 4 + 5 + 6 + 7 + 9,$$
$$34 = 1 + 3 + 4 + 5 + 6 + 7 + 8.$$

Atque ex his natura serierum, quae hoc pacto pro litteris α, β, γ, δ etc. prodeunt, facile perspicitur.

19. Investigando igitur, quot variis modis quisque numerus in partes inaequales numero datas distribui possit, series istae litteris α, β, γ, δ etc. signatae formari poterunt, quod autem opus foret summopere molestum. Vicissim autem ex his seriebus aliunde cognitis et formatis resolvi poterit problema hoc non inelegans, quod mihi a Viro Clar. NAUDEO[1]) propositum ita se habet:

Definire, quot variis modis datus numerus produci queat ex additione aliquot numerorum integrorum inter se inaequalium, quorum numerus detur.

Sic Clariss. Propositor quaerit, quot variis modis numerus 50 oriri possit ex additione septem numerorum integrorum inaequalium. Ad quam quaestionem resolvendam manifestum est in subsidium vocari debere seriem η, in

---

1) Vide epistolam a PH. NAUDÉ minore (1684—1747) ad EULERUM datam 4. Calendas Septembris 1740, *LEONHARDI EULERI Opera omnia*, series III. F. R.

qua coefficiens cuiusque termini indicat, quot variis modis exponens ipsius n resolvi possit in 7 partes inaequales. Quare series illa

$$\eta = n^{28} + n^{29} + 2n^{30} + 3n^{31} + 5n^{32} + 7n^{33} + 11n^{34} + \text{etc.}$$

continuari debebit usque ad terminum, in quo potestas quinquagesima ipsius n continetur, cuius coefficiens, qui erit 522, ostendet numerum 50 omnino 522 modis diversis ex additione septem numerorum integrorum inter se inaequalium produci posse. Ex quo perspicuum est, si modus habeatur commodus et facilis formandi illas series α, β, γ, δ etc., eo ipso problema istud NAUDEANUM perfectissime solutum iri.

20. Cum igitur supra (§ 5 et 9) modus traditus sit inveniendi valores litterarum α, β, γ, δ etc. ex cognitis valoribus litterarum A, B, C, D etc., in praesenti negotio resolutionem facile expedire poterimus, propterea quod ex § 17 cognitos habemus valores A, B, C, D etc.; atque praeterea est, ut sequitur,

$$\alpha = A,$$

$$\beta = \frac{\alpha A - B}{2},$$

$$\gamma = \frac{\beta A - \alpha B + C}{3},$$

$$\delta = \frac{\gamma A - \beta B + \alpha C - D}{4},$$

$$\varepsilon = \frac{\delta A - \gamma B + \beta C - \alpha D + E}{5}$$

etc.

Ex his igitur obtinebimus

$$\alpha = \frac{n}{1-n},$$

$$2\beta = \frac{\alpha n}{1-n} - \frac{nn}{1-nn},$$

$$3\gamma = \frac{\beta n}{1-n} - \frac{\alpha n^2}{1-n^2} + \frac{n^3}{1-n^3},$$

$$4\delta = \frac{\gamma n}{1-n} - \frac{\beta n^2}{1-n^2} + \frac{\alpha n^3}{1-n^3} - \frac{n^4}{1-n^4}$$

etc.

Quodsi autem loco α, β, γ etc. successive substituantur valores ante reperti, prodibunt

$$\alpha = \frac{n}{1-n},$$

$$\beta = \frac{n^3}{(1-n)(1-nn)},$$

$$\gamma = \frac{n^6}{(1-n)(1-nn)(1-n^3)},$$

$$\delta = \frac{n^{10}}{(1-n)(1-n^2)(1-n^3)(1-n^4)},$$

$$\varepsilon = \frac{n^{15}}{(1-n)(1-n^2)(1-n^3)(1-n^4)(1-n^5)}$$

etc.

Ex his itaque intelligitur esse in hoc casu

$$\alpha = A,$$

$$\beta = AB,$$

$$\gamma = ABC,$$

$$\delta = ABCD,$$

$$\varepsilon = ABCDE$$

etc.

21. Lex haec, qua valores litterarum α, β, γ, δ etc. progredi sunt inventi, compluribus formulis evolutis observatur eiusque veritas nisi per inductionem adhuc non constat. Quo igitur haec veritas firmius confirmetur, conveniet eandem progressionis legem alio modo planissimo, in quo inductioni nullus locus relinquatur, elicere. Cum itaque nobis propositum sit valores litterarum α, β, γ, δ etc. indagare, quos sortiuntur in serie

$$R = 1 + \alpha z + \beta z^2 + \gamma z^3 + \delta z^4 + \varepsilon z^5 + \text{etc.},$$

si fuerit, uti initio assumsimus,

$$R = (1 + nz)(1 + n^2 z)(1 + n^3 z)(1 + n^4 z)\ldots,$$

notandum est, si loco z scribatur nz, expressionem, cui modo R erat aequalis, mutari in hanc formam

$$(1+n^2z)(1+n^3z)(1+n^4z)(1+n^5z)\ldots,$$

quae multiplicata per $1+nz$ ipsam priorem expressionem producit. Quamobrem recte concludimus, si in serie

$$1+\alpha z+\beta z^2+\gamma z^3+\delta z^4+\varepsilon z^5+\text{etc.}$$

loco z scribamus nz, ut habeamus

$$1+\alpha nz+\beta n^2z^2+\gamma n^3z^3+\delta n^4z^4+\varepsilon n^5z^5+\text{etc.},$$

hancque expressionem per $1+nz$ multiplicemus, tum productum, quod erit

$$\begin{aligned}1+\alpha nz&+\beta n^2z^2+\gamma n^3z^3+\delta n^4z^4+\varepsilon n^5z^5+\text{etc.}\\ +\ nz&+\alpha n^2z^2+\beta n^3z^3+\gamma n^4z^4+\delta n^5z^5+\text{etc.},\end{aligned}$$

aequale esse debere illi ipsi priori seriei

$$1+\alpha z+\beta z^2+\gamma z^3+\delta z^4+\varepsilon z^5+\text{etc.}$$

Quodsi ergo actu coefficientes terminorum homologorum coaequemus, nanciscemur sequentes pro α, β, γ etc. determinationes

$$\begin{aligned}\alpha&=\frac{n}{1-n}=\frac{n}{1-n},\\ \beta&=\frac{\alpha n^2}{1-n^2}=\frac{n^3}{(1-n)(1-n^2)},\\ \gamma&=\frac{\beta n^3}{1-n^3}=\frac{n^6}{(1-n)(1-n^2)(1-n^3)},\\ \delta&=\frac{\gamma n^4}{1-n^4}=\frac{n^{10}}{(1-n)(1-n^2)(1-n^3)(1-n^4)}\\ &\text{etc.}\end{aligned}$$

22. Hoc igitur modo invenimus summas serierum illarum α, β, γ, δ etc. satis commode expressas, ex quibus vicissim ipsae illae series formari poterunt. Nam cum illae series secundum potestates ipsius n progrediantur, eae prodire

debebunt, si istae expressiones summarum per divisionem more consueto evolvantur atque in series infinitas secundum potestates ipsius n procedentes convertantur. Quae operatio cum divisione absolvatur, manifestum est omnes illas series α, β, γ, δ etc. ad id genus pertinere, quod nomine serierum recurrentium indicari solet; atque adeo quilibet terminus ex aliquot praecedentibus determinabitur. Ut autem pateat, quomodo in singulis his seriebus quisque terminus ex praecedentibus sit formandus, denominatores illarum expressionum pro litteris α, β, γ, δ etc. inventarum per multiplicationem actu evolvi debent, quo facto habebitur

$$\alpha = \frac{n}{1-n},$$

$$\beta = \frac{n^3}{1-n-n^2+n^3},$$

$$\gamma = \frac{n^6}{1-n-n^2+n^4+n^5-n^6},$$

$$\delta = \frac{n^{10}}{1-n-n^2+2n^5-n^8-n^9+n^{10}},$$

$$\varepsilon = \frac{n^{15}}{1-n-n^2+n^5+n^6+n^7-n^8-n^9-n^{10}+n^{13}+n^{14}-n^{15}},$$

$$\zeta = \frac{n^{21}}{1-n-n^2+n^5+2n^7-n^9-n^{10}-n^{11}-n^{12}+2n^{14}+n^{16}-n^{19}-n^{20}+n^{21}}$$

etc.

Atque ex his denominatoribus intelligitur, quomodo in singulis seriebus quisque terminus ex praecedentibus componi debeat, si praecepta, quae de formatione serierum recurrentium habentur, in subsidium vocentur.

23. At ex forma expressionum pro litteris α, β, γ, δ etc. inventarum, qua quaelibet est productum ex praecedente in novum quempiam factorem, alius deducitur modus satis idoneus ex quavis serie iam inventa seriem sequentem inveniendi. Sic, cum series $\alpha = \frac{n}{1-n}$ sit progressio geometrica

$$\alpha = n + n^2 + n^3 + n^4 + n^5 + n^6 + n^7 + \text{etc.},$$

ex hac reperietur series β, si ea multiplicetur per $\frac{n^2}{1-n^2}$, vel si multiplicetur per hanc progressionem geometricam

$$n^2 + n^4 + n^6 + n^8 + n^{10} + n^{12} + n^{14} + \text{etc.}$$

Ex serie porro β hoc pacto inventa, si ea multiplicetur per

$$\frac{n^3}{1-n^3} = n^3 + n^6 + n^9 + n^{12} + n^{15} + n^{18} + \text{etc.},$$

producetur series γ. Haecque multiplicata per

$$\frac{n^4}{1-n^4} = n^4 + n^8 + n^{12} + n^{16} + n^{20} + n^{24} + \text{etc.}$$

producet seriem δ. Atque ita porro seriem cuiusque ordinis multiplicando per certam quandam progressionem geometricam reperietur series sequens. Hocque pacto non difficulter has series, quousque libuerit, continuare licebit; atque sic problema supra memoratum a Clar. NAUDEO propositum resolvetur.

24. Facilius autem quaelibet series ex se ipsa ope praecedentis poterit continuari, si ad modum respiciamus, quo valor cuiusque litterarum α, β, γ, δ etc. ex praecedente determinatur. Sic, cum sit $\beta = \frac{\alpha n^2}{1-n^2}$, erit $\beta = \beta nn + \alpha nn$; quare si ad seriem β per nn multiplicatam addatur series α per nn multiplicata, ipsa series β oriri debebit. Cum igitur constet seriei β primum terminum esse n^3, ponamus

$$\beta = \mathfrak{a}n^3 + \mathfrak{b}n^4 + \mathfrak{c}n^5 + \mathfrak{d}n^6 + \mathfrak{e}n^7 + \mathfrak{f}n^8 + \mathfrak{g}n^9 + \text{etc.}$$

eritque

$$\beta n^2 = \qquad + \mathfrak{a}n^5 + \mathfrak{b}n^6 + \mathfrak{c}n^7 + \mathfrak{d}n^8 + \mathfrak{e}n^9 + \text{etc.},$$

$$\alpha n^2 = n^3 + n^4 + n^5 + n^6 + n^7 + n^8 + n^9 + \text{etc.}$$

Aequatis iam terminis propter $\beta = \beta nn + \alpha nn$ habebimus

$$\begin{aligned} \mathfrak{a} &= 1, & \mathfrak{e} &= \mathfrak{c} + 1 = 3, \\ \mathfrak{b} &= 1, & \mathfrak{f} &= \mathfrak{d} + 1 = 3, \\ \mathfrak{c} &= \mathfrak{a} + 1 = 2, & \mathfrak{g} &= \mathfrak{e} + 1 = 4, \\ \mathfrak{d} &= \mathfrak{b} + 1 = 2, & \mathfrak{h} &= \mathfrak{f} + 1 = 4 \end{aligned}$$

etc.

Simili modo, cum sit $\gamma = \frac{\beta n^3}{1-n^3}$ seu $\gamma = \gamma n^3 + \beta n^3$, ex serie β formabitur series γ atque porro ex serie γ ope aequationis $\delta = \delta n^4 + \gamma n^4$ producetur series δ; pariterque sequentes omnes conficientur.

25. Quoniam in expressione

$$R = 1 + \alpha z + \beta z^2 + \gamma z^3 + \delta z^4 + \text{etc.}$$

valores litterarum α, β, γ, δ etc. invenimus sitque

$$R = (1 + nz)(1 + n^2 z)(1 + n^3 z)(1 + n^4 z) \ldots,$$

convertetur productum hoc ex infinitis factoribus constans

$$(1 + nz)(1 + n^2 z)(1 + n^3 z)(1 + n^4 z) \ldots$$

in seriem hanc secundum potestates ipsius z procedentem

$$1 + \frac{nz}{1-n} + \frac{n^3 z^2}{(1-n)(1-n^2)} + \frac{n^6 z^3}{(1-n)(1-n^2)(1-n^3)} + \frac{n^{10} z^4}{(1-n)(1-n^2)(1-n^3)(1-n^4)} + \text{etc.}$$

Atque summae huius seriei logarithmus hyperbolicus ex § 10 erit

$$= \frac{nz}{1-n} - \frac{nnz^2}{2(1-n^2)} + \frac{n^3 z^3}{3(1-n^3)} - \frac{n^4 z^4}{4(1-n^4)} + \text{etc.}$$

Vel si k scribatur pro numero, cuius logarithmus $= 1$, erit

$$k^{\frac{nz}{1-n} - \frac{n^2 z^2}{2(1-n^2)} + \frac{n^3 z^3}{3(1-n^3)} - \frac{n^4 z^4}{4(1-n^4)} + \text{etc.}} = R$$

seu ista expressio exponentialis est aequalis summae illius seriei, in quam valorem ipsius R transmutavimus.

26. Verum ut ad propositum problema revertamur, quo definiendum sit, quot variis modis datus numerus m partiri queat in μ partes inaequales inter se et integras, indicemus hunc modorum numerum, quem quaerimus, huiusmodi scriptione

$$m^{(\mu)i},$$

qua nobis perpetuo numerus modorum indicetur, quibus numerus m per additionem produci queat ex μ numeris integris inter se inaequalibus; atque ad hanc partium inaequalitatem denotandam supra litteram i adiunximus, quae omittetur, si quaestio formabitur de numero modorum inveniendo, quibus datus numerus m omnino in μ partes tam aequales quam inaequales distribui queat. Quod problema postea pari facilitate solutum exhibebitur.

27. Iste ergo modorum numerus $m^{(\mu)i}$ erit coefficiens potestatis n^m in illa serierum α, β, γ, δ, ε etc., quae a prima α numerata in ordine est tota, quot μ continet unitates. Huius seriei summa est

$$= \frac{n^{\frac{\mu(\mu+1)}{1\cdot 2}}}{(1-n)(1-n^2)(1-n^3)(1-n^4)\cdots(1-n^\mu)}$$

ideoque seriei, quae ex hac forma nascitur, terminus generalis est $= m^{(\mu)i} n^m$. Seriei autem, quae nascitur ex hac forma

$$\frac{n^{\frac{\mu(\mu-1)}{1\cdot 2}}}{(1-n)(1-n^2)(1-n^3)(1-n^4)\cdots(1-n^\mu)},$$

terminus generalis erit $= m^{(\mu)i} n^{m-\mu}$ seu pro eadem ipsius n potestate erit terminus generalis $= (m+\mu)^{(\mu)i} n^m$. Subtrahatur prior expressio a posteriore atque residuae expressionis

$$\frac{n^{\frac{\mu(\mu-1)}{1\cdot 2}}}{(1-n)(1-n^2)(1-n^3)(1-n^4)\cdots(1-n^{\mu-1})}$$

terminus generalis erit $= n^m((m+\mu)^{(\mu)i} - m^{(\mu)i})$; huius autem eiusdem seriei terminus generalis est $m^{(\mu-1)i} n^m$, quocirca habebimus

$$m^{(\mu-1)i} = (m+\mu)^{(\mu)i} - m^{(\mu)i},$$

unde hanc adipiscimur regulam, ut sit

$$(m+\mu)^{(\mu)i} = m^{(\mu)i} + m^{(\mu-1)i},$$

cuius ope, si constiterit, quot variis modis numerus m distribui possit cum in μ partes tum in $\mu - 1$ partes inaequales, hos binos modorum numeros addendo reperietur, quot variis modis numerus maior $m + \mu$ distribui possit in μ partes inaequales. Atque ita resolutio casuum difficiliorum ad simpliciores reducitur atque tandem ad simplicissimos per se notos; quippe constat, si fuerit $m < \frac{\mu\mu+\mu}{2}$, tum fore $m^{(\mu)i} = 0$, et si fuerit $m = \frac{\mu\mu+\mu}{2}$, tum erit $m^{(\mu)i} = 1$.

28. Cum formula $m^{(\mu)i} n^m$ sit terminus generalis huius expressionis

$$\frac{n^{\frac{\mu(\mu+1)}{2}}}{(1-n)(1-n^2)(1-n^3)\cdots(1-n^\mu)},$$

videamus, qualem seriem praebeat ista expressio

$$\frac{1}{(1-n)(1-n^2)(1-n^3)\cdots(1-n^\mu)},$$

si evolvatur atque secundum dimensiones ipius n disponatur. Ponamus autem prodire hanc seriem

$$1+pn+qn^2+rn^3+sn^4+tn^5+\text{etc.}^{1)},$$

ex cuius generatione perspicitur coefficientem cuiusque potestatis ipsius n monstrare, quot variis modis exponens ipsius n per additionem produci queat ex his datis numeris

$$1,\quad 2,\quad 3,\quad 4,\quad 5,\quad 6,\ \ldots\ \mu;$$

hicque nec certus partium numerus praescribitur, ex quibus componatur, nec ista conditio ponitur, ut partes sint inter se inaequales. Hanc itaque ob causam expressio $m^{(\mu)\prime}$ simul indicabit, quot variis omnino modis numerus $m-\frac{\mu(\mu+1)}{2}$ per additionem produci queat ex numeris $1, 2, 3, 4, 5, \ldots \mu$. Sic si quaeratur, quot variis modis numerus 50 distribui possit in 7 partes inaequales, propter $m=50$ et $\mu=7$ quaestio eo reducitur, ut investigetur, quot variis modis numerus $50-28$ seu 22 oriri queat per additionem ex his septem numeris 1, 2, 3, 4, 5, 6, 7. Hoc ergo pacto duplicis generis quaestiones una eademque opera resolvuntur.

29. Definitis hoc pacto litteris α, β, γ, δ etc. pro casu, quo loco litterarum a, b, c, d etc. progressionem geometricam n, n^2, n^3, n^4, n^5 etc. infinitam assumsimus, ordo postulat, ut etiam in valores tertii ordinis $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, $\mathfrak{E}$ etc. inquiramus. Adhibuimus autem has litteras $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ etc. in seriebus his valoribus $\frac{1}{R}$ et $\frac{1}{S}$ aequalibus; sumsimus enim supra (§ 11) esse

$$\frac{1}{S}=1+\mathfrak{A}z+\mathfrak{B}z^2+\mathfrak{C}z^3+\mathfrak{D}z^4+\mathfrak{E}z^5+\text{etc.}$$

et

$$\frac{1}{R}=1-\mathfrak{A}z+\mathfrak{B}z^2-\mathfrak{C}z^3+\mathfrak{D}z^4-\mathfrak{E}z^5+\text{etc.}$$

1) Editio princeps: $1+\alpha n+\beta n^2+2n^3+n^4+n^5+\text{etc.}$ F. R.

obtinentibus R et S valores primum assumtos, quibus erat

$$R = (1 + nz)(1 + n^2z)(1 + n^3z)(1 + n^4z) \text{ etc.},$$
$$S = (1 - nz)(1 - n^2z)(1 - n^3z)(1 - n^4z) \text{ etc.}$$

Intelligitur autem hinc seriem $\frac{1}{S} = 1 + \mathfrak{A}z + \mathfrak{B}z^2 + \mathfrak{C}z^3 + \mathfrak{D}z^4 + \text{etc.}$ oriri, si innumerabiles istae progressiones geometricae in se invicem multiplicentur

$$\frac{1}{1 - nz} = 1 + nz + n^2z^2 + n^3z^3 + n^4z^4 + \text{etc.},$$
$$\frac{1}{1 - n^2z} = 1 + n^2z + n^4z^2 + n^6z^3 + n^8z^4 + \text{etc.},$$
$$\frac{1}{1 - n^3z} = 1 + n^3z + n^6z^2 + n^9z^3 + n^{12}z^4 + \text{etc.},$$
$$\frac{1}{1 - n^4z} = 1 + n^4z + n^8z^2 + n^{12}z^3 + n^{16}z^4 + \text{etc.}$$
$$\text{etc.}$$

Posito autem $-z$ loco z prodit simili modo series $\frac{1}{R}$.

30. Ex ista harum serierum generatione manifestum est esse:

$$\text{I.} \quad \mathfrak{A} = n + n^2 + n^3 + n^4 + n^5 + \text{etc.},$$

quae est progressio geometrica omnes ipsius n potestates complectens singulas per coefficientem $+1$ multiplicatas.

$$\text{II.} \quad \mathfrak{B} = n^2 + n^3 + 2n^4 + 2n^5 + 3n^6 + 3n^7 + 4n^8 + 4n^9 + \text{etc.},$$

in qua coefficiens cuiusque ipsius n potestatis tot continet unitates, quot variis modis exponens ipsius n in duas partes sive aequales sive inaequales partiri potest. Sic potestatis n^8 coefficiens est 4, quia 8 quatuor modis in 2 partes partitur

$$8 = 1 + 7, \quad 8 = 2 + 6, \quad 8 = 3 + 5, \quad 8 = 4 + 4.$$

$$\text{III.} \quad \mathfrak{C} = n^3 + n^4 + 2n^5 + 3n^6 + 4n^7 + 5n^8 + 7n^9 + \text{etc.},$$

in qua cuiusque potestatis ipsius n coefficiens tot continet unitates, quot variis

modis exponens ipsius n in tres partes sive aequales sive inaequales distribui potest. Sic n^9 coefficientem habet 7, quia 7 modis 9 in tres partes dispertiri se patitur:

$$9 = 1 + 1 + 7, \quad 9 = 1 + 4 + 4,$$
$$9 = 1 + 2 + 6, \quad 9 = 2 + 2 + 5,$$
$$9 = 1 + 3 + 5, \quad 9 = 2 + 3 + 4,$$
$$9 = 3 + 3 + 3.$$

$$\text{IV.} \quad \mathfrak{D} = n^4 + n^5 + 2n^6 + 3n^7 + 5n^8 + 6n^9 + 9n^{10} + \text{etc.},$$

ubi cuiusque potestatis ipsius n coefficiens tot continet unitates, quot variis modis exponens ipsius n in quatuor partes sive aequales sive inaequales resolvi potest. Atque similis est ratio sequentium serierum, quae pro litteris $\mathfrak{E}$, $\mathfrak{F}$, $\mathfrak{G}$ etc. reperiuntur.

31. Harum ergo serierum ope alterum problema, quod simul cum praecedente Vir Cl. NAUDEUS[1]) mihi proposuit, resolvi potest, quod ita se habet:

Invenire, quot variis modis datus numerus m partiri possit in μ partes tam aequales quam inaequales, sive invenire, quot variis modis datus numerus m per additionem μ numerorum integrorum sive aequalium sive inaequalium produci queat.

Quod problema a praecedente eo tantum discrepat, quod in praecedente partitio ad partes tantum inter se inaequales sit restricta, haec autem partes quoque aequales admittat. Ad numerum autem omnium modorum in hoc problemate quaesitum signo exprimendum utamur hac forma

$$m^{(\mu)},$$

quae scilicet declaret, quot variis modis numerus m partiri queat in μ partes integras partium aliquot aequalitate non exclusa; quamobrem in signo supra affixo (μ) ante adnexa littera i, qua inaequalitas partium indicabatur, hic est praetermissa.

32. Solutio ergo huius problematis ad formationem serierum $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, $\mathfrak{E}$ etc. reducitur; at supra iam ostendimus (§ 5), quomodo harum litterarum

1) Vide notam p. 178. F. R.

valores ex valoribus litterarum α, β, γ, δ etc. iam cognitis definiantur. Quanquam autem iste modus est generalis et ex rei natura petitus, tamen non satis dilucide legem, qua hi valores progrediuntur, ob oculos ponit. Quamobrem valores harum litterarum $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, $\mathfrak{E}$ etc. via huic casui propria investigabo, simili ei, qua supra (§ 21) usus sum.

Quoniam est

$$\frac{1}{S} = \frac{1}{(1-nz)(1-n^2z)(1-n^3z)(1-n^4z)\text{ etc.}},$$

perspicuum est, si in hac forma loco z scribatur nz, tum prodituram esse hanc formam

$$\frac{1}{(1-n^2z)(1-n^3z)(1-n^4z)(1-n^5z)\text{ etc.}}.$$

Ad ipsam autem hanc formam prior $\frac{1}{S}$ perducitur, si ea multiplicetur per $1-nz$. Hanc ob rem, cum assumserimus esse

$$\frac{1}{S} = 1 + \mathfrak{A}z + \mathfrak{B}z^2 + \mathfrak{C}z^3 + \mathfrak{D}z^4 + \mathfrak{E}z^5 + \text{etc.},$$

ponamus in hac nz loco z habebimusque

$$1 + \mathfrak{A}nz + \mathfrak{B}n^2z^2 + \mathfrak{C}n^3z^3 + \mathfrak{D}n^4z^4 + \text{etc.}$$

Iam priorem seriem $\frac{1}{S}$ multiplicemus per $1-nz$

$$\begin{aligned} 1 + \mathfrak{A}z + {} & \mathfrak{B}z^2 + \mathfrak{C}z^3 + \mathfrak{D}z^4 + \text{etc.} \\ - nz - {} & \mathfrak{A}nz^2 - \mathfrak{B}nz^3 - \mathfrak{C}nz^4 - \text{etc.} \end{aligned}$$

Quae forma cum illi esse debeat aequalis, erit

$$\mathfrak{A} = \frac{n}{1-n} = \frac{n}{1-n},$$

$$\mathfrak{B} = \frac{\mathfrak{A}n}{1-n^2} = \frac{n^2}{(1-n)(1-n^2)},$$

$$\mathfrak{C} = \frac{\mathfrak{B}n}{1-n^3} = \frac{n^3}{(1-n)(1-n^2)(1-n^3)},$$

$$\mathfrak{D} = \frac{\mathfrak{C}n}{1-n^4} = \frac{n^4}{(1-n)(1-n^2)(1-n^3)(1-n^4)}$$

etc.

33. Hinc igitur nova percipitur relatio inter valores litterarum $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ etc. et litterarum α, β, γ, δ etc., quae eo magis est notatu digna, quo minus hi valores a se invicem discrepant. Collato enim § 21 intelligitur esse

$$\begin{aligned} \alpha &= \mathfrak{A}, \\ \beta &= n\ \mathfrak{B}, \\ \gamma &= n^3\ \mathfrak{C}, \\ \delta &= n^6\ \mathfrak{D}, \\ \varepsilon &= n^{10}\mathfrak{E} \\ &\text{etc.} \end{aligned}$$

Manifestum ergo est ratione coefficientium series $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ etc. omnino cum seriebus α, β, γ, δ etc. congruere totumque discrimen in exponentibus ipsius n situm esse. In serie quidem $\mathfrak{A}$ exponentes quoque aequales sunt exponentibus in serie α, at in serie $\mathfrak{B}$ exponentes unitate deficiunt ab exponentibus seriei β, in serie $\mathfrak{C}$ exponentes ternario deficiunt ab exponentibus seriei γ, et ita porro defectus secundum numeros trigonales progrediuntur.

34. Ex seriebus ergo α, β, γ, δ etc., quas supra formare docuimus et quibus prius problema NAUDEANUM resolvitur, simul hoc posterius problema a NAUDEO propositum ita resolvi potest, ut eius solutio reducatur ad solutionem prioris. Erit nempe

$$\begin{aligned} m^{(1)} &= m^{(1)\prime}, \\ m^{(2)} &= (m+1)^{(2)\prime}, \\ m^{(3)} &= (m+3)^{(3)\prime}, \\ m^{(4)} &= (m+6)^{(4)\prime} \end{aligned}$$

et generaliter

$$m^{(\mu)} = \left(m + \frac{\mu(\mu-1)}{2}\right)^{(\mu)\prime}$$

et vicissim

$$m^{(\mu)\prime} = \left(m - \frac{\mu(\mu-1)}{2}\right)^{(\mu)}.$$

Quoniam autem porro invenimus [§ 27] esse

$$(m+\mu)^{(\mu)\prime} = m^{(\mu)\prime} + m^{(\mu-1)\prime},$$

erit reductione ad casum praesentem facta

$$\left(m-\frac{\mu(\mu-3)}{2}\right)^{(\mu)}=\left(m-\frac{\mu(\mu-1)}{2}\right)^{(\mu)}+\left(m-\frac{(\mu-1)(\mu-2)}{2}\right)^{(\mu-1)}$$

seu commodius

$$m^{(\mu)}=(m-\mu)^{(\mu)}+(m-1)^{(\mu-1)},$$

ex qua proprietate etiam facile series litterarum $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. formabuntur, sicque hoc alterum problema resolvetur.

35. Ad exemplum huius problematis quaestionem Vir Clar. affert, ut determinetur, quot variis modis numerus 50 in septem omnino partes sive aequales sive inaequales dispertiri queat. Haec ergo quaestio ad prius problema reducetur, ob $m=50$ et $\mu=7$, si quaeratur, quot variis modis numerus $50+21$ seu numerus 71 in septem partes inaequales partiri queat. Utrumque autem fieri potest 8946 modis diversis. Praeterea vero hic idem numerus 8946 indicat (§ 28), quot variis modis $71-28=43$ per additionem produci queat ex his numeris 1, 2, 3, 4, 5, 6, 7. Atque generaliter numerus modorum $m^{(\mu)}$, quibus numerus m in μ partes sive aequales sive inaequales resolvitur, simul ostendit, quot variis modis numerus $m-\mu$ produci queat per additionem ex his numeris definitis

$$1,\ 2,\ 3,\ 4,\ 5,\ \ldots\ \mu.$$

36. Finem huic dissertationi faciat observatio notatu digna, quam quidem rigore geometrico demonstrare mihi nondum licuit. Observavi scilicet hoc infinitorum factorum productum

$$(1-n)(1-n^2)(1-n^3)(1-n^4)(1-n^5) \text{ etc.},$$

si per multiplicationem actu evolvatur, praebere hanc seriem

$$1-n-n^2+n^5+n^7-n^{12}-n^{15}+n^{22}+n^{26}-n^{35}-n^{40}+n^{51}+\text{etc.}$$ [1]),

1) Haec series, quae apud EULERUM primum hac in Commentatione 158 (exhib. d. 6. Apr. 1741), deinde vero etiam in huius voluminis Commentationibus 175, 191, 243, 244 (ubi evolutionis demonstratio datur) nec non in EULERI *Introductione* (vide notam p. 163) invenitur, eo magis digna est, quae consideretur, quod iam exemplum praebet illarum functionum, quas centum

ubi eae tantum ipsius n potestates occurrunt, quarum exponentes continentur hac forma $\frac{3xx \pm x}{2}$. Ac si x sit numerus impar, potestates ipsius n, quae sunt $n^{\frac{3xx \pm x}{2}}$, coefficientem habent -1; si autem x sit numerus par, tum potestates $n^{\frac{3xx \pm x}{2}}$ coefficientem habent $+1$.

37. Praeterea notari meretur series huius reciproca, quae oritur ex evolutione huius fractionis

$$\frac{1}{(1-n)(1-n^2)(1-n^3)(1-n^4)(1-n^5)\text{ etc.}};$$

prodibit scilicet ista series recurrens

$$1 + 1n + 2n^2 + 3n^3 + 5n^4 + 7n^5 + 11n^6 + 15n^7 + 22n^8 + \text{etc.},$$

quippe quae per seriem superiorem

$$1 - n - n^2 + n^5 + n^7 - n^{12} - n^{15} + n^{22} + n^{26} - \text{etc.}$$

fere abhinc annos C. G. J. JACOBI ut fundamenta theoriae functionum ellipticarum in analysin introduxit et hoc charactere ϑ significavit. In epistola a. 1848 ad P. H. FUSS data JACOBI scripsit: „Ich möchte mir bei dieser Gelegenheit noch erlauben, Ihnen zu sagen, warum ich mich so sehr für diese EULERSCHE Entdeckung interessiere. Sie ist nämlich der erste Fall gewesen, in welchem Reihen aufgetreten sind, deren Exponenten eine arithmetische Reihe *zweiter* Ordnung bilden, und auf diese Reihen ist durch mich die Theorie der elliptischen Transcendenten gegründet worden. Die EULERSCHE Formel ist ein spezieller Fall einer Formel, welche wohl das wichtigste und fruchtbarste ist, was ich in reiner Mathematik erfunden habe . . .;" vide P. STÄCKEL und W. AHRENS, *Der Briefwechsel zwischen C. G. J. JACOBI und P. H. VON FUSS über die Herausgabe der Werke LEONHARD EULERS*, Leipzig 1908, p. 60 (nec non p. 23 et 42). Vide etiam C. G. J. JACOBI, *Elementarer Beweis einer merkwürdigen analytischen Formel, nebst einigen aus ihr folgenden Zahlensätzen*, Journal f. d. reine u. angew. Mathem. 21, 1840, p. 13; *C. G. J. JACOBIS Gesammelte Werke*, Bd. 6, p. 281. Cf. quoque epistolas a DAN. BERNOULLIO d. 28. Jan. 1741 et 14. Apr. 1742 ad EULERUM datas, *Correspondance math. et phys. publiée par P. H. Fuss*, St.-Pétersbourg 1843, t. II, p. 466 et 490, porro epistolam, quam EULERUS d. 15. Oct. 1743 ad GOLDBACH scripsit, ibidem t. I, p. 258, atque epistolas ab EULERO d. 1. Sept. et 10. Nov. 1742 ad NIC. BERNOULLIUM datas, *LEONHARDI EULERI Opera postuma*, t. I, p. 521 et 528; *LEONHARDI EULERI Opera omnia*, series III. Vide praeterea P. STÄCKEL, *Ein Brief EULERS an D'ALEMBERT*, Biblioth. Mathem. 11_3, 1910/1, p. 220. Vide autem etiam G. ENESTROEM, *JACOB BERNOULLI und die JACOBISCHE Thetafunktion*, Biblioth. Mathem. 9_3, 1908/9, p. 206, et L. SCHLESINGER, *Über GAUSS' Arbeiten zur Funktionentheorie*, Nachrichten v. d. Königl. Gesellsch. d. Wissensch zu Göttingen, Math.-phys. Klasse 1912, Beiheft, p. 8—10. F. R.

multiplicata producit unitatem. In illa autem serie coefficiens cuiusque potestatis ipsius n tot continet unitates, quot variis modis exponens ipsius n in partes dispertiri potest; sic 5 septem modis in partes resolvi potest, uti

$$5 = 5, \qquad 5 = 3 + 2, \qquad 5 = 2 + 2 + 1,$$
$$5 = 4 + 1, \qquad 5 = 3 + 1 + 1, \qquad 5 = 2 + 1 + 1 + 1,$$
$$5 = 1 + 1 + 1 + 1 + 1;$$

nec numerus scilicet partium hic praescribitur nec inaequalitas.

THEOREMATA CIRCA DIVISORES NUMERORUM IN HAC FORMA $paa \pm qbb$ CONTENTORUM[1])

Commentatio 164 indicis ENESTROEMIANI
Commentarii academiae scientiarum Petropolitanae **14** (1744/6), 1751, p. 151—181

In sequentibus theorematis litterae a et b designant numeros quoscunque integros primos inter se seu qui praeter unitatem nullum alium habeant divisorem communem.

THEOREMA 1

Numerorum in hac forma $aa + bb$ *contentorum divisores primi omnes sunt vel* 2 *vel huius formae* $4m + 1$ *numeri.*

---

1) Ad haec theoremata, quae EULERUS „magnam partem ex sola inductione conclusit" hicque sine demonstratione proposuit, primo consulendae sunt Commentationes 134, 228, 241, 242, 256, 262, 271, 272 huius voluminis, deinde vero praecipue hae duae (598 et 610 indicis ENESTROEMIANI): *De insigni promotione scientiae numerorum, Opuscula analytica* **2**, 1785, p. 275, et *Novae demonstrationes circa divisores numerorum formae* $xx + nyy$, Nova acta acad. sc. Petrop. **1** (1783), 1787, p. 47; *LEONHARDI EULERI Opera omnia*, series I, vol. 4. Vide autem etiam I. L. LAGRANGE, *Recherches d'arithmétique*, Nouv. mém. de l'acad. d. sc. de Berlin (1773), 1775, p. 265, et (1775), 1777, p. 323; *Oeuvres de LAGRANGE*, publiées par les soins de M. I.-A. SERRET, t. III, p. 695.

Theoremata sequentia et annotationes ad ea pertinentes eo magis considerari merentur, quod in summa iam continent elegantissimum illud theorema, cui C. F. GAUSS in *Disquisitionibus arithmeticis* nomen *theorematis fundamentalis* dedit — „quia omnia fere, quae de residuis quadraticis dici possunt, huic theoremati innituntur". Vide notam p. 217. F. R.

THEOREMA 2

Omnes numeri primi huius formae $4m+1$ *vicissim in hac numerorum formula* $aa+bb$ *continentur.*

THEOREMA 3

Summa ergo duorum quadratorum seu numerus huius formae $aa+bb$ *dividi nequit per ullum numerum huius formae* $4m-1$.

THEOREMA 4

Numerorum in hac forma $aa+2bb$ *contentorum divisores primi omnes sunt vel* 2 *vel numeri in hac forma* $8m+1$ *vel in hac* $8m+3$ *contenti.*

THEOREMA 5

Omnes numeri primi in hac forma $8m+1$ *vel* $8m+3$ *contenti vicissim sunt numeri huius formae* $aa+2bb$.

THEOREMA 6

Nullus numerus huius formae $aa+2bb$ *dividi potest per ullum numerum huius formae* $8m-1$ *vel huius* $8m-3$.

THEOREMA 7

Numerorum in hac forma $aa+3bb$ *contentorum divisores primi omnes sunt vel* 2 *vel* 3 *vel in una harum formularum* $12m+1$, $12m+7$ *contenti.*

THEOREMA 8

Omnes numeri primi in alterutra harum formularum $12m+1$ *vel* $12m+7$ *sive in hac una* $6m+1$ *contenti simul sunt numeri huius formae* $aa+3bb$.

THEOREMA 9

Nullus numerus sive huius formulae $12m-1$ *sive huius* $12m-7$, *hoc est nullus numerus huius formae* $6m-1$, *est divisor ullius numeri in hac forma* $aa+3bb$ *contenti.*

THEOREMA 10

Numerorum in hac forma $aa+5bb$ *contentorum divisores primi omnes sunt vel* 2 *vel* 5 *vel in una harum* 4 *formarum* $20m+1$, $20m+3$, $20m+7$, $20m+9$ *contenti.*

THEOREMA 11

Si fuerint numeri $20m+1$, $20m+3$, $20m+9$, $20m+7$ *primi, tum erit, ut sequitur:*

$$20m+1=aa+5bb,\quad 2(20m+3)=aa+5bb,$$

$$20m+9=aa+5bb,\quad 2(20m+7)=aa+5bb.$$

THEOREMA 12

Nullus numerus in una sequentium formularum contentus $20m-1$, $20m-3$, $20m-9$, $20m-7$ *potest esse divisor ullius numeri huius formae* $aa+5bb$.

THEOREMA 13

Numerorum in hac forma $aa+7bb$ *contentorum divisores primi omnes sunt vel* 2 *vel* 7 *vel in una sequentium*

sex formularum		*seu in una harum trium*
$28m+1$,	$28m+11$,	$14m+1$,
$28m+9$,	$28m+15$,	$14m+9$,
$28m+25$,	$28m+23$	$14m+11$

sunt contenti.

THEOREMA 14

Si fuerint numeri in istis formulis $14m+1$, $14m+9$, $14m+11$ *contenti primi, tum simul in hac forma* $aa+7bb$ *continentur.*

THEOREMA 15

Nullus numerus huius formae $aa+7bb$ *potest dividi per ullum numerum, qui in una sequentium*

sex formularum		*seu harum trium*
$28m+3$,	$28m+5$,	$14m+3$,
$28m+13$,	$28m+17$,	$14m+5$,
$28m+19$,	$28m+27$	$14m+13$

contineatur.

THEOREMA 16

Numerorum in hac forma $aa+11bb$ *contentorum omnes divisores primi sunt vel* 2 *vel* 11 *vel continentur in una sequentium*

10 *formularum*		*seu* 5 *formularum*
$44m+1$,	$44m+3$,	$22m+1$,
$44m+9$,	$44m+27$,	$22m+3$,
$44m+37$,	$44m+23$,	$22m+9$,
$44m+25$,	$44m+31$,	$22m+5$,
$44m+5$,	$44m+15$	$22m+15$.

THEOREMA 17

Si fuerint numeri in his sive decem sive quinque formulis contenti primi, tum simul erunt vel ipsi vel eorum quadrupli numeri huius formae $aa+11bb$.

THEOREMA 18

Nullus numerus huius formae $aa + 11bb$ *potest dividi per ullum numerum, qui contineatur in una sequentium*

sive 10 *formularum*		*sive* 5 *formularum*
$44m + 7$,	$44m + 29$,	$22m + 7$,
$44m + 13$,	$44m + 35$,	$22m + 13$,
$44m + 17$,	$44m + 39$,	$22m + 17$,
$44m + 19$,	$44m + 41$,	$22m + 19$,
$44m + 21$,	$44m + 43$	$22m + 21$.

THEOREMA 19

Numerorum in hac forma $aa + 13bb$ *contentorum omnes divisores primi sunt vel* 2 *vel* 13 *vel continentur in una sequentium* 12 *formularum*

$52m + 1$,	$52m + 7$,
$52m + 49$,	$52m + 31$,
$52m + 9$,	$52m + 11$,
$52m + 25$,	$52m + 19$,
$52m + 29$,	$52m + 47$,
$52m + 17$,	$52m + 15$.

THEOREMA 20

Omnes numeri primi, qui in priori formularum istarum columna continentur, simul sunt numeri huius formae $aa + 13bb$. *Numerorum autem primorum, qui in altera formularum columna continentur, dupla sunt numeri formae* $aa + 13bb$.

THEOREMA 21

Nullus numerus huius formae $aa + 13bb$ *dividi potest per ullum numerum, qui contineatur in una sequentium formularum*

$$\begin{array}{ll} 52m + 3, & 52m + 35, \\ 52m + 5, & 52m + 37, \\ 52m + 21, & 52m + 41, \\ 52m + 23, & 52m + 43, \\ 52m + 27, & 52m + 45, \\ 52m + 33, & 52m + 51. \end{array}$$

THEOREMA 22

Numerorum in hac forma $aa + 17bb$ *contentorum omnes divisores primi sunt vel* 2 *vel* 17 *vel in una sequentium formularum continentur*

$$\begin{array}{ll} 68m + 1, & 68m + 3, \\ 68m + 9, & 68m + 27, \\ 68m + 13, & 68m + 39, \\ 68m + 49, & 68m + 11, \\ 68m + 33, & 68m + 31, \\ 68m + 25, & 68m + 7, \\ 68m + 21, & 68m + 63, \\ 68m + 53, & 68m + 23. \end{array}$$

THEOREMA 23

Omnes numeri primi, qui in priori harum formularum columna continentur, ad quos 2 *referri debet, sunt formae* $aa + 17bb$, *vel ipsi quidem vel eorum noncupla. Numerorum autem primorum in altera columna contentorum tripla sunt numeri formae* $aa + 17bb$.

THEOREMA 24

Nullus numerus huius formae $aa + 17bb$ *dividi potest per ullum numerum, qui contineatur in aliqua sequentium formularum*

$68m - 1$,	$68m - 3$,
$68m - 9$,	$68m - 27$,
$68m - 13$,	$68m - 39$,
$68m - 49$,	$68m - 11$,
$68m - 33$,	$68m - 31$,
$68m - 25$,	$68m - 7$,
$68m - 21$,	$68m - 63$,
$68m - 53$,	$68m - 23$.

THEOREMA 25

Numerorum in hac forma $aa + 19bb$ *contentorum omnes divisores primi sunt vel* 2 *vel* 19 *vel continentur in una sequentium*

18 *formularum*		*vel harum* 9
$76m + 1$,	$76m + 5$,	$38m + 1$,
$76m + 25$,	$76m + 49$,	$38m + 5$,
$76m + 17$,	$76m + 9$,	$38m + 7$,
$76m + 45$,	$76m + 73$,	$38m + 9$,
$76m + 61$,	$76m + 7$,	$38m + 11$,
$76m + 35$,	$76m + 23$,	$38m + 17$,
$76m + 39$,	$76m + 43$,	$38m + 23$,
$76m + 63$,	$76m + 11$,	$38m + 25$,
$76m + 55$,	$76m + 47$	$38m + 35$.

THEOREMA 26

Omnes numeri primi, qui in una harum formularum continentur, sunt vel ipsi vel saltem quater sumti numeri huius formae $aa + 19bb$.

THEOREMA 27

Nullus numerus huius formae $aa + 19bb$ *dividi potest per ullum numerum, qui contineatur in aliqua sequentium 9 formularum*

$$\begin{array}{lll} 38m - 1, & 38m - 9, & 38m - 23, \\ 38m - 5, & 38m - 11, & 38m - 25, \\ 38m - 7, & 38m - 17, & 38m - 35. \end{array}$$

His igitur theorematis continetur indoles formularum $aa + qbb$, si q fuerit numerus primus; ac primum quidem vidimus omnes divisores primos huiusmodi formularum esse vel 2 vel q vel in talibus expressionibus $4qm + \alpha$ ita comprehendi posse, ut nullus divisor in iis non contineatur, tum vero, ut omnis numerus primus $4qm + \alpha$ simul sit divisor formulae cuiusdam $aa + qbb$. Deinde etiam hoc colligere licet, si numerus primus formae $4qm + \alpha$ fuerit divisor cuiusquam numeri $aa + qbb$, tum nullum numerum formae $4qm - \alpha$ divisorem esse posse eiusdem expressionis $aa + qbb$. Cum igitur inter formas divisorum formulae $aa + qbb$ semper contineatur haec $4mq + 1$, manifestum est nullum numerum $aa + qbb$ dividi posse per ullum numerum formae $4mq - 1$. Denique attendenti manifestum fiet, si q fuerit numerus primus formae $4n - 1$, tum divisorum formas ad numerum duplo minorem redigi posse, ita ut ad formulas $2qm + \alpha$ revocari queant, quod fieri nequit, si q sit numerus primus formae $4n + 1$. Si igitur pro hac forma $aa + (4n + 1)bb$ divisor fuerit $4(4n + 1)m + \alpha$, tum nullus numerus formae istius

$$4(4n + 1)m + 2(4n + 1) + \alpha$$

poterit esse divisor eiusdem expressionis $aa + (4n + 1)bb$. Plures annotationes faciemus, cum etiam formulas $aa + qbb$, quando q non est numerus primus, fuerimus contemplati.

THEOREMA 28

Numerorum in hac forma $aa+6bb$ *vel hac* $2aa+3bb$ *contentorum divisores primi omnes sunt vel 2 vel 3 vel in una sequentium formularum continentur*

$$24m+1,\qquad 24m+7,$$
$$24m+5,\qquad 24m+11.$$

THEOREMA 29

Omnes numeri primi formae vel $24m+1$ *vel* $24m+7$ *continentur in expressione* $aa+6bb$; *at numeri primi istam formam* $24m+5$ *et* $24m+11$ *habentes continentur in expressione* $2aa+3bb$.

THEOREMA 30

Nullus numerus sive $aa+6bb$ *sive* $2aa+3bb$ *dividi potest per ullum numerum, qui contineatur in aliqua harum formularum*

$$24m-1,\qquad 24m-5,$$
$$24m-7,\qquad 24m-11.$$

THEOREMA 31

Numerorum in hac $aa+10bb$ *vel hac forma* $2aa+5bb$ *contentorum divisores primi omnes sunt vel 2 vel 5 vel in una sequentium formularum continentur*

$$40m+1,\qquad 40m+7,$$
$$40m+9,\qquad 40m+23,$$
$$40m+11,\qquad 40m+37,$$
$$40m+19,\qquad 40m+13.$$

THEOREMA 32

Numeri primi in priori harum formularum columna contenti simul sunt numeri huius formae $aa+10bb$; *et numeri primi in altera columna contenti sunt numeri huius formae* $2aa+5bb$.

THEOREMA 33

Nullus numerus sive huius formae $aa + 10bb$ *sive huius* $2aa + 5bb$ *dividi potest per ullum numerum, qui in aliqua sequentium formularum contineatur*

$40m - 1$,	$40m - 7$,
$40m - 9$,	$40m - 23$,
$40m - 11$,	$40m - 37$,
$40m - 19$,	$40m - 13$.

THEOREMA 34

Numerorum in hac forma $aa + 14bb$ *vel hac* $2aa + 7bb$ *contentorum divisores primi omnes sunt vel* 2 *vel* 7 *vel in una sequentium formularum continentur*

$56m + 1$,	$56m + 3$,
$56m + 9$,	$56m + 27$,
$56m + 25$,	$56m + 19$,
$56m + 15$,	$56m + 5$,
$56m + 23$,	$56m + 45$,
$56m + 39$,	$56m + 13$.

THEOREMA 35

Numeri primi in priori harum formularum columna contenti simul sunt numeri vel huius formae $aa + 14bb$ *vel* $2aa + 7bb$; *qui autem in altera columna continentur, eorum tripla demum in altera istarum formularum comprehenduntur.*

THEOREMA 36

Si in superioribus formulis signa $+$ *in* $-$ *commutentur, tum nullus numerus in istis formulis contentus divisor erit vel formae* $aa + 14bb$ *vel* $2aa + 7bb$.

26*

THEOREMA 37

Numerorum in hac forma $aa + 15bb$ *vel hac* $3aa + 5bb$ *contentorum divisores primi omnes sunt vel* 2 *vel* 3 *vel* 5 *vel in una sequentium formularum continentur*

		vel harum 4
$60m + 1$,	$60m + 31$,	$30m + 1$,
$60m + 17$,	$60m + 47$,	$30m + 17$,
$60m + 19$,	$60m + 49$,	$30m + 19$,
$60m + 23$,	$60m + 53$	$30m + 23$.

THEOREMA 38

Numerorum in hac forma $aa + 21bb$ *vel hac* $3aa + 7bb$ *contentorum divisores primi omnes sunt vel* 2 *vel* 3 *vel* 7 *vel in una sequentium formularum continentur*

$84m + 1$,	$84m + 5$,
$84m + 25$,	$84m + 41$,
$84m + 37$,	$84m + 17$,
$84m + 55$,	$84m + 11$,
$84m + 31$,	$84m + 23$,
$84m + 19$,	$84m + 71$.

THEOREMA 39

Numerorum in hac forma $aa + 35bb$ *vel* $5aa + 7bb$ *contentorum divisores primi omnes sunt vel* 2 *vel* 5 *vel* 7 *vel in una sequentium formularum continentur*

		vel harum
$140m + 1$,	$140m + 3$,	$70m + 1$,
$140m + 9$,	$140m + 27$,	$70m + 3$,
$140m + 81$,	$140m + 103$,	$70m + 9$,
$140m + 29$,	$140m + 87$,	$70m + 11$,
$140m + 121$,	$140m + 83$,	$70m + 13$,
$140m + 109$,	$140m + 47$,	$70m + 17$,
$140m + 11$,	$140m + 33$,	$70m + 27$,
$140m + 99$,	$140m + 17$,	$70m + 29$,
$140m + 51$,	$140m + 13$,	$70m + 33$,
$140m + 39$,	$140m + 117$,	$70m + 39$,
$140m + 71$,	$140m + 73$,	$70m + 47$,
$140m + 79$,	$140m + 97$	$70m + 51$.

THEOREMA 40

Numerorum in aliqua harum formularum contentorum

$$aa + 30bb, \quad 2aa + 15bb,$$
$$3aa + 10bb, \quad 5aa + 6bb$$

divisores primi omnes sunt vel 2 vel 3 vel 5 vel in una sequentium formularum continentur

$120m + 1$,	$120m + 11$,
$120m + 13$,	$120m + 23$,
$120m + 49$,	$120m + 59$,
$120m + 37$,	$120m + 47$,
$120m + 17$,	$120m + 67$,
$120m + 101$,	$120m + 31$,
$120m + 113$,	$120m + 43$,
$120m + 29$,	$120m + 79$.

Theoremata haec sufficiunt ad sequentes annotationes formandas, ex quibus natura divisorum huiusmodi formularum $paa + qbb$ penitius perspicietur.[1])

ANNOTATIO 1

Formula $paa + qbb$ nullum habet divisorem, quin sit simul divisor formulae $aa + pqbb$. Cuius quidem rei ratio facile patet; nam qui numerus est divisor formulae $paa + qbb$, idem dividet hanc formam $ppaa + pqbb$, hoc est hanc $aa + pqbb$ posito a loco pa. Hanc ob rem sufficiet istam unicam formam $aa + Nbb$ considerasse, quippe quae ratione divisorum hanc $paa + qbb$ in se complectitur.

ANNOTATIO 2

Inter numeros primos, qui ullum numerum in hac formula $aa + Nbb$ contentum dividunt, primum occurrit binarius. Si enim N sit numerus impar, sumendis pro a et b numeris imparibus formula $aa + Nbb$ fiet per 2 divisibilis; at si N sit numerus par, sumto a pari formula quoque per 2 fit divisibilis. Deinde vero ipse numerus N vel quaelibet eius pars aliquota poterit esse divisor formulae $aa + Nbb$, quod sumendo $a = N$ est perspicuum.

ANNOTATIO 3

Reliqui divisores primi omnes formulae $aa + Nbb$ in istiusmodi expressionibus $4Nm + \alpha$ comprehendi possunt, ita ut etiam vicissim omnes numeri primi in formis istis $4Nm + \alpha$ contenti simul sint divisores formulae $aa + Nbb$. Praeterea si expressio $4Nm + \alpha$ praebeat divisores formulae $aa + Nbb$, tum nullus numerus huiusmodi $4Nm - \alpha$ poterit esse divisor ullius numeri in formula $aa + Nbb$ contenti.

ANNOTATIO 4

Habebit autem α certos quosdam valores, qui ab indole numeri N pendebunt; ac semper quidem unitas erit unus ex valoribus ipsius α. Tum vero, quia de numeris primis in formula $4Nm + \alpha$ contentis quaestio est, perspicuum est neque ullum numerum parem neque ullum numerum, qui cum N communem habeat divisorem, valorem ipsius α constituere posse.

1) Ad sequentes annotationes praecipue consulendae sunt EULERI Commentationes 242 et 598 supra (nota p. 194) laudatae. F. R.

ANNOTATIO 5

Valores autem ipsius α omnes erunt minores quam $4N$; si enim qui essent maiores, per diminutionem numeri m minores quam $4N$ reddi possent. Hinc valores ipsius α erunt numeri impares minores quam $4N$ atque ad N primi. Neque vero omnes istiusmodi numeri impares ad N primi idoneos pro α valores exhibebunt, sed eorum semissis ab hoc officio excluditur, quoniam, si x fuerit valor ipsius α, tum $-x$ seu $4N-x$ eius valor esse nequit; vicissimque si x non fuerit valor ipsius α, tum $4N-x$ certo eius valor sit futurus.

ANNOTATIO 6

Numerus igitur valorum ipsius α, ita ut $4Nm+\alpha$ contineat omnes divisores primos formulae $aa+Nbb$, sequenti modo definietur.[1]) Sint p, q, r, s etc. numeri primi inter se diversi excepto binario, qui seorsim est considerandus, atque

si fuerit	erit valorum ipsius α numerus
$N=1$,	1,
$N=2$,	2,
$N=p$,	$p-1$,
$N=2p$,	$2(p-1)$,
$N=pq$,	$(p-1)(q-1)$,
$N=2pq$,	$2(p-1)(q-1)$,
$N=pqr$,	$(p-1)(q-1)(r-1)$,
$N=2pqr$	$2(p-1)(q-1)(r-1)$
etc.,	etc.

ANNOTATIO 7

Quemadmodum autem unitas semper reperitur inter valores ipsius α, ita etiam quivis numerus quadratus impar et primus ad N locum habere debet in valoribus ipsius α. Posito enim b numero pari $2c$ formula fiet $aa+4Ncc$, quae, si sit numerus primus, contineri debet in expressione $4Nm+\alpha$. Ergo α erit aa vel residuum, quod ex divisione ipsius aa per $4N$ remanet. Simili modo inter valores ipsius α reperiri debent omnes numeri $aa+N$ vel quae

1) Vide Commentationem 271 huius voluminis. F. R.

ex eorum per $4N$ divisione supererunt residua; posito enim $b = 2c + 1$ fiet $aa + Nbb = aa + N + 4N(cc + c)$; qui si fuerit numerus primus, debebit $aa + N$ esse valor ipsius α.

ANNOTATIO 8

Intelligitur etiam, si x fuerit valor ipsius α, tum quoque xx (quod quidem ex praecedente patet) et omnes omnino potestates ipsius x, puta x^μ, inter valores ipsius α locum habere debere. Deinde si praeter x quoque y fuerit valor ipsius α, tum quoque xy et generaliter $x^\mu y^\nu$ dabit quoque valorem ipsius α. Scilicet si $x^\mu y^\nu$ maius fuerit quam $4N$, per hoc dividatur et residuum erit valor ipsius α. Simili modo si insuper z fuerit valor ipsius α, tum etiam $x^\mu y^\nu z^\xi$ erit valor ipsius α. Hincque ex cognito uno vel aliquot valoribus ipsius α facili negotio omnes omnino eius valores inveniuntur.

ANNOTATIO 9

Sit x quicunque numerus primus ad $4N$ eoque minor atque vel $+x$ vel. $-x$ valor erit ipsius α. Si igitur fuerit x numerus primus, ex sequenti tabula intelligetur, quibus casibus $+x$ quibusque $-x$ valorem ipsius α praebeat:

Si	erit
$N = 3n - 1$	$\alpha = +3$
$N = 3n + 1$	$\alpha = -3$
$N = \begin{cases} 5n + 1 \\ 5n + 4 \end{cases}$	$\alpha = +5$
$N = \begin{cases} 5n + 2 \\ 5n + 3 \end{cases}$	$\alpha = -5$
$N = \begin{cases} 7n + 3 \\ 7n + 5 \\ 7n + 6 \end{cases}$	$\alpha = +7$
$N = \begin{cases} 7n + 1 \\ 7n + 2 \\ 7n + 4 \end{cases}$	$\alpha = -7$

si	erit
$N = \begin{cases} 11n + 2 \\ 11n + 6 \\ 11n + 7 \\ 11n + 8 \\ 11n + 10 \end{cases}$	$\alpha = +11$
$N = \begin{cases} 11n + 1 \\ 11n + 3 \\ 11n + 4 \\ 11n + 5 \\ 11n + 9 \end{cases}$	$\alpha = -11$

Si propositus sit numerus quicunque primus, qui utrum signo $+$ an $-$ affectus valorem ipsius α praebeat, ita investigabitur: Bini casus debent evolvi, alter, quo propositus numerus primus est formae $4u+1$, alter, quo est formae $4u-1$. Priori casu erit $\alpha = +(4u+1)$, si fuerit $N = (4u+1)n + tt$, at $\alpha = -(4u+1)$, si fuerit $N \mathrel{\not=} (4u+1)n + tt$. Posteriori casu autem erit $\alpha = +(4u-1)$, si sit $N \mathrel{\not=} (4u-1)n + tt$, at $\alpha = -(4u-1)$, si $N = (4u-1)n + tt$. Ubi notandum est, quemadmodum signum $=$ aequalitatem denotat, ita signum $\mathrel{\not=}$ aequalitatis impossibilitatem designare. Quodsi autem fuerit pro utroque casu $N = (4u \pm 1)n + s$, erit quoque $N = (4u \pm 1)n + s^{\nu}$ denotante ν numerum quemcunque integrum, unde ista tabella pro quibusvis numeris primis sine negotio construitur.

ANNOTATIO 10

Quoniam inter formas divisorum primorum ipsius $aa + Nbb$ habetur $4Nm + 1$, eadem expressio $aa + Nbb$ per nullum numerum dividi poterit, qui contineatur in hac forma $4Nm - 1$. Simili modo cum $4Nm + tt$ exhibeat formam divisorum expressionis $aa + Nbb$, sequitur nullum numerum huiusmodi $4Nm - tt$ posse esse divisorem ullius numeri in hac forma $aa + Nbb$ contenti, siquidem, quod semper pono, a et b sint numeri inter se primi. Hanc ob rem impossibilis erit ista aequatio $(4Nm - tt)u = aa + Nbb$ ideoque erit $4Nmu - ttu - Nbb \mathrel{\not=} aa$, siquidem fuerint $4Nmu - ttu$ et Nbb numeri inter se primi; quod cum certo eveniat, si $b = 1$ et $t = 1$, nanciscimur istud

CONSECTARIUM

Nullus numerus hac formula $4abc - b - c$ *contentus unquam esse potest quadratus.*

ANNOTATIO 11

Si fuerit N numerus huius formae $4n - 1$, tum formae divisorum ad numerum duplo minorem rediguntur, ita ut in formulis $2Nm + \alpha$ comprehendantur. Scilicet si fuerit $4Nm + \alpha$ divisorum forma, tum quoque $4Nm + 2N + \alpha$ erit forma divisorum. Quare cum $2Nm + tt$ sit forma divisorum, sequitur nullum numerum $2Nm - tt$ divisorem esse posse formae $aa + Nbb$. Hinc erit $(2Nm - tt)u \neq aa + Nbb$ existente $N = 4n - 1$, unde oritur hoc

CONSECTARIUM

Nullus numerus huius formae $2abc - b - c$, *si vel* b *vel* c *fuerit numerus impar* $4n - 1$, *unquam potest esse quadratus.*

ANNOTATIO 12

Si fuerit N numerus impar huiusmodi $4n + 1$ vel etiam numerus impariter par, tum divisorum formae ad numerum duplo minorem redigi non possunt. Scilicet si $4Nm + \alpha$ fuerit divisor formae $aa + Nbb$, tum $4Nm + 2N + \alpha$ eiusdem formae divisor esse non poterit. Hinc $2(2m + 1)N + tt$ non erit divisor formae $aa + Nbb$ ideoque haec aequatio $(2(2m + 1)N + tt)u = aa + Nbb$ erit aequatio impossibilis, siquidem sint a et b numeri primi inter se et N sit vel numerus impar formae $4n + 1$ vel numerus impariter par. Ex quo sequitur istud

CONSECTARIUM

Nullus numerus huius formae $2abc - b + c$ *existente* a *numero impari et* b *vel impariter pari vel impari formae* $4n + 1$ *unquam esse potest quadratus.*

SCHOLION 1

Quae hic sunt allata, sufficienter declarant indolem divisorum huiusmodi formularum $aa + Nbb$ simulque inserviunt ad omnes divisorum formas ex-

pedite inveniendas, quibus cognitis quoque eae numerorum formae innotescunt, quae nunquam praebere queant divisores formulae $aa + Nbb$. Cum igitur haec pateant ad omnes valores ipsius N, sive sint numeri primi sive compositi, reliquum est, ut etiam casus evolvamus, quibus N denotet numeros negativos tam primos quam compositos; perspicuum autem est formulam $paa - qbb$ nullum divisorem habere posse, quin sit divisor huius $aa - pqbb$ seu $pqaa - bb$, unde sufficiet huiusmodi tantum formas $aa - Nbb$ evolvisse.

THEOREMA 41

Numerorum in hac forma $aa - bb$ contentorum divisores primi omnes sunt vel 2 vel $4m \pm 1$; nullus scilicet datur numerus, qui non sit divisor differentiae duorum quadratorum. Vicissim autem omnes numeri praeter impariter pares ipsi sunt differentiae duorum quadratorum.

THEOREMA 42

Numerorum in hac forma $aa - 2bb$ contentorum omnes divisores primi sunt vel 2 vel huius formae $8m \pm 1$. Omnesque numeri primi huius formae $8m \pm 1$ ipsi infinitis modis in formula $aa - 2bb$ continentur.

THEOREMA 43

Numerorum in hac forma contentorum $aa - 3bb$ omnes divisores primi sunt vel 2 vel 3 vel huius formae $12m \pm 1$. Atque vicissim omnes huiusmodi numeri primi simul in hac forma $aa - 3bb$ vel hac $3aa - bb$ infinitis modis continentur.

THEOREMA 44

Omnes divisores primi huius formae $aa - 5bb$ sunt vel 2 vel 5 vel continentur

in altera harum formularum	*vel in hac una*
$20m \pm 1, \quad 20m \pm 9$	$10m \pm 1.$

Omnesque numeri primi in his formis contenti simul sunt divisores formae $aa - 5bb$.

THEOREMA 45

Omnes divisores primi huius formae $aa - 7bb$ *sunt vel* 2 *vel* 7 *vel in una sequentium formularum continentur*

$$28m \pm 1, \quad 28m \pm 3, \quad 28m \pm 9;$$

atque vicissim omnes numeri primi in his formis contenti simul sunt divisores formae $aa - 7bb$.

THEOREMA 46

Omnes divisores primi huius formae $aa - 11bb$ *sunt vel* 2 *vel* 11 *vel in una sequentium formarum continentur*

$$44m \pm 1, \quad 44m \pm 5, \quad 44m \pm 7, \quad 44m \pm 9, \quad 44m \pm 19;$$

atque vicissim omnes numeri primi in his formulis contenti simul sunt divisores formae $aa - 11bb$, *quae reciprocatio in omnibus sequentibus theorematis locum habet.*

THEOREMA 47

Omnes divisores primi formae $aa - 13bb$ *sunt vel* 2 *vel* 13 *vel in sequentibus formulis continentur*

		quae revocantur ad has
$52m \pm 1$,	$52m \pm 3$,	$26m \pm 1$,
$52m \pm 9$,	$52m \pm 25$,	$26m \pm 3$,
$52m \pm 23$,	$52m \pm 17$,	$26m \pm 9$.

THEOREMA 48

Omnes divisores primi numerorum huius formae $aa - 17bb$ *sunt vel* 2 *vel* 17 *vel in sequentibus formulis continentur*

		quae revocantur ad has
$68m \pm 1$,	$68m \pm 9$,	$34m \pm 1$,
$68m \pm 13$,	$68m \pm 19$,	$34m \pm 9$,
$68m \pm 33$,	$68m \pm 25$,	$34m \pm 13$,
$68m \pm 21$,	$68m \pm 15$,	$34m \pm 15$.

THEOREMA 49

Omnes divisores primi numerorum huius formae $aa - 19bb$ *sunt vel* 2 *vel* 19 *vel in sequentibus formulis continentur*

$$76m \pm 1, \quad 76m \pm 3, \quad 76m \pm 9,$$
$$76m \pm 27, \quad 76m \pm 5, \quad 76m \pm 15,$$
$$76m \pm 31, \quad 76m \pm 17, \quad 76m \pm 25.$$

THEOREMA 50

Omnes divisores primi numerorum formae huius $aa - 6bb$ *sunt vel* 2 *vel* 3 *vel in his formulis continentur*

$$24m \pm 1, \quad 24m \pm 5.$$

THEOREMA 51

Omnes divisores primi numerorum formae $aa - 10bb$ *sunt vel* 2 *vel* 5 *vel in his formulis continentur*

$$40m \pm 1, \quad 40m \pm 3,$$
$$40m \pm 9, \quad 40m \pm 13.$$

THEOREMA 52

Omnes divisores primi numerorum huius formae $aa - 14bb$ *sunt vel* 2 *vel* 7 *vel in his formulis continentur*

$$56m \pm 1, \quad 56m \pm 5, \quad 56m \pm 25,$$
$$56m \pm 13, \quad 56m \pm 9, \quad 56m \pm 11.$$

THEOREMA 53

Omnes divisores primi numerorum huius formae $aa-22bb$ *sunt vel* 2 *vel* 11 *vel in his formulis continentur*

$88m\pm1,\quad 88m\pm3,\quad 88m\pm9,$
$88m\pm27,\quad 88m\pm7,\quad 88m\pm21,$
$88m\pm25,\quad 88m\pm13,\quad 88m\pm39,$
$88m\pm29.$

THEOREMA 54

Omnes divisores primi numerorum huius formae $aa-15bb$ *sunt vel* 2 *vel* 3 *vel* 5 *vel in his formulis continentur*

$60m\pm1,\quad 60m\pm7,\quad 60m\pm11,\quad 60m\pm17.$

THEOREMA 55

Omnes divisores primi numerorum huius formae $aa-21bb$ *sunt vel* 2 *vel* 3 *vel* 7 *vel in his formulis continentur*

		quae revocantur ad has
$84m\pm1,$	$84m\pm5,$	$42m\pm1,$
$84m\pm25,$	$84m\pm41,$	$42m\pm5,$
$84m\pm37,$	$84m\pm17,$	$42m\pm17.$

THEOREMA 56

Omnes divisores primi numerorum huius formae $aa-33bb$ *sunt vel* 2 *vel* 3 *vel* 11 *vel in his formulis continentur*

		quae revocantur ad has
$132m\pm1,$	$132m\pm17,$	$66m\pm1,$
$132m\pm25,$	$132m\pm29,$	$66m\pm17,$
$132m\pm35,$	$132m\pm65,$	$66m\pm25,$
$132m\pm49,$	$132m\pm41,$	$66m\pm29,$
$132m\pm37,$	$132m\pm31,$	$66m\pm31.$

THEOREMA 57

Omnes divisores primi numerorum huius formae $aa - 35bb$ *sunt vel* 2 *vel* 5 *vel* 7 *vel in his formulis continentur*

$140m \pm 1,$	$140m \pm 9,$	$140m \pm 59,$
$140m \pm 29,$	$140m \pm 19,$	$140m \pm 31,$
$140m \pm 13,$	$140m \pm 23,$	$140m \pm 67,$
$140m \pm 43,$	$140m \pm 33,$	$140m \pm 17.$

THEOREMA 58

Omnes divisores primi numerorum huius formae $aa - 30bb$ *sunt vel* 2 *vel* 3 *vel* 5 *vel in his formulis continentur*

$120m \pm 1,$	$120m \pm 13,$	$120m \pm 49,$
$120m \pm 37,$	$120m \pm 7,$	$120m \pm 29,$
$120m \pm 17,$	$120m \pm 19.$	

THEOREMA 59

Omnes divisores primi numerorum huius formae $aa - 105bb$ *sunt vel* 2 *vel* 3 *vel* 5 *vel* 7 *vel continentur in his formulis*

		quae revocantur ad has
$420m \pm 1,$	$420m \pm 13,$	$210m \pm 1,$
$420m \pm 169,$	$420m \pm 97,$	$210m \pm 13,$
$420m \pm 23,$	$420m \pm 121,$	$210m \pm 23,$
$420m \pm 107,$	$420m \pm 131,$	$210m \pm 41,$
$420m \pm 109,$	$420m \pm 157,$	$210m \pm 53,$
$420m \pm 59,$	$420m \pm 73,$	$210m \pm 59,$
$420m \pm 101,$	$420m \pm 53,$	$210m \pm 73,$
$420m \pm 151,$	$420m \pm 137,$	$210m \pm 79,$
$420m \pm 89,$	$420m \pm 103,$	$210m \pm 89,$
$420m \pm 79,$	$420m \pm 187,$	$210m \pm 97,$
$420m \pm 41,$	$420m \pm 113,$	$210m \pm 101,$
$420m \pm 209,$	$420m \pm 197,$	$210m \pm 103.$

ANNOTATIO 13

Numerorum ergo in formula $aa - Nbb$ contentorum divisores primi omnes sunt vel 2 vel divisores numeri N vel in eiusmodi formulis $4Nm \pm \alpha$ comprehenduntur. Quodsi enim $4Nm + \alpha$ fuerit forma divisorum, tum quoque $4Nm - \alpha$ erit divisorum forma; secus atque in formulis $aa + Nbb$; quarum si $4Nm + \alpha$ fuerit divisor, tum $4Nm - \alpha$ nullum unquam praebere potest divisorem eiusdem formulae.

ANNOTATIO 14

Posito ergo $4Nm \pm \alpha$ pro forma divisorum generali numerorum in hac expressione $aa - Nbb$ contentorum littera α plerumque plures significabit numeros, inter quos unitas semper continetur; tum vero, quia hic de divisoribus primis sermo est, inter valores ipsius α nullus erit numerus par nec ullus divisor numeri N. Deinde etiam manifestum est omnes valores ipsius α ita ordinari posse, ut sint minores quam $2N$. Si enim sit $4Nm + 2N + b$ divisor, tum posito $m - 1$ loco m divisor erit $4Nm - (2N - b)$. Erunt ergo valores ipsius α numeri impares primi ad N minores quam $2N$ horumque numerorum omnium imparium et primorum ad N et minorum quam $2N$ semissis tantum praebebit idoneos valores ipsius α; reliqui exhibebunt formulas, in quibus plane nullus continetur divisor. Perpetuo scilicet totidem habebuntur formulae divisorum, quot sunt contrariae, solo excepto casu, quo $N = 1$.

ANNOTATIO 15

Quod ad numerum valorum ipsius α pro formula divisorum $4Nm \pm \alpha$ attinet, quoniam ob signum ambiguum quaevis formula est duplex, hic quoque eadem valebit regula, quam supra Annotatione 6 dedi. Sic in ultimo theoremate, quo erat $N = 105 = 3 \cdot 5 \cdot 7$, numerus valorum ipsius α erit $= 2 \cdot 4 \cdot 6 = 48$, seu cum quaevis formula sit gemina, numerus formularum fit 24, quot etiam exhibuimus.

ANNOTATIO 16

Sicut autem unitas perpetuo inter valores ipsius α reperitur, ita etiam quivis numerus quadratus, qui sit primus ad $4N$, valorem idoneum pro α

suppeditabit.[1]) Posito enim $b = 2c$ formula $aa - Nbb$ abit in $aa - 4Ncc$ seu $4Ncc - aa$, ex quo patet quemvis numerum quadratum aa, qui sit primus ad $4N$, exhibere valorem idoneum pro α, sumendo scilicet residuo, quod in divisione ipsius aa per $4N$ remanet. Simili modo ponendo $b = 2c + 1$ formula $Nbb - aa$ abit in $4N(cc + c) + N - aa$, unde etiam omnes numeri $N - aa$ seu $aa - N$, qui quidem sint primi ad $4N$, idoneos valores pro α praebebunt. Deinde quoque notandum est, si sint x, y, z valores ipsius α, tum quoque x^μ, y^ν, z^ζ itemque omnia producta, quae ex numeris x, y, z eorumve potestatibus quibuscunque resultant, valores ipsius α esse exhibitura; unde cognito uno vel aliquot valoribus ipsius α facili negotio omnes reperiuntur.

ANNOTATIO 17

Quo autem clarius appareat, cuiusmodi valores littera α perpetuo sit habitura, tabulam sequentem adiicere visum est, similem eius, quae Annotatione 9 habetur.

Erit scilicet	si fuerit
$\alpha = 3$	$N = 3n + 1$
$\alpha \,\overline{\perp}\, 3$	$N = 3n - 1$

1) His EULERI verbis L. KRONECKER in Commentatione, quae inscribitur *Bemerkungen zur Geschichte des Reciprocitätsgesetzes*, Monatsber. d. Akad. d. Wissensch. zu Berlin (1875), 1876, p. 267, *L. KRONECKERS Werke*, herausgegeben von K. HENSEL, Bd. 2, Leipzig 1897, p. 4, sequentia adiecit:

„Nimmt man nun die einfache Bemerkung hinzu, daß für eine Primzahl N schon die ersten $\frac{1}{2}(N-1)$ ungraden Quadratzahlen, da sie mod. N unter einander inkongruent sind, so viel geeignete Werte (valores idoneos) für α liefern, als nach EULER überhaupt erforderlich sind, so ergibt sich unmittelbar das Reciprocitätsgesetz; denn es folgt alsdann, daß N quadratischer Rest von jeder Primzahl sein muß — aber auch nur von einer solchen —, welche, positiv oder negativ genommen, einem Quadrate mod. $4N$ kongruent ist.

EULER selbst hat das Reciprocitätsgesetz in ganz entwickelter und vollendeter Form erst viel später und zwar am Schlusse einer Abhandlung aufgestellt, welche er unter dem Titel *Observationes circa divisionem quadratorum per numeros primos* im I. Bande seiner *Opuscula analytica* (Petersburg 1783) publiciert hat.“

Dissertatio a KRONECKER hic laudata est EULERI Commentatio 552 (indicis ENESTROEMIANI), *LEONHARDI EULERI Opera omnia*, series I, vol. 3. F. R.

erit scilicet	si fuerit
$\alpha = 5$	$N = 5n \begin{cases} +1 \\ -1 \end{cases}$
α ⌶ 5	$N = 5n \begin{cases} +2 \\ -2 \end{cases}$
$\alpha = 7$	$N = 7n \begin{cases} +1 \\ +2 \\ -3 \end{cases}$
α ⌶ 7	$N = 7n \begin{cases} -1 \\ -2 \\ +3 \end{cases}$
$\alpha = 11$	$N = 11n \begin{cases} +1 \\ -2 \\ +3 \\ +4 \\ +5 \end{cases}$
α ⌶ 11	$N = 11n \begin{cases} -1 \\ +2 \\ -3 \\ -4 \\ -5 \end{cases}$
$\alpha = 13$	$N = 13n \begin{cases} +1 \\ -1 \\ +3 \\ -3 \\ +4 \\ -4 \end{cases}$
α ⌶ 13	$N = 13n \begin{cases} +2 \\ -2 \\ +5 \\ -5 \\ +6 \\ -6 \end{cases}$

ANNOTATIO 18

Ex hac igitur tabula numeri primi, qui idoneos valores pro α praebeant, facile dignosci simulque inepti reiici possunt. Proposito scilicet numero primo p omnes numeri quadrati in huiusmodi formulis $pn + \theta$ comprehendi possunt, quae prodeunt ponendo pro θ numeros quadratos seu residua, quae ex divisione quadratorum per p remanent. Quare si N fuerit huiusmodi numerus $pn + tt$, tum inter formas divisorum $4Nm \pm \alpha$ formulae $aa - Nbb$ seu $Nbb - aa$ habebitur $\alpha = p$; sin autem numerus N non contineatur in forma $pn + tt$, tum nullus numerus in formula hac $4Nm \pm p$ contentus poterit esse divisor ullius numeri huius formae $aa - Nbb$.

ANNOTATIO 19

Si fuerit N numerus impar formae $4n + 1$, tum expressionis $aa - Nbb$ divisorum formae $4Nm \pm \alpha$ ad duplo pauciores reduci possunt, ita ut exhiberi possint hoc modo $2Nm \pm \alpha$. Hoc scilicet casu, si $4Nm \pm \alpha$ fuerit forma divisorum, tum quoque $4Nm \pm (2N - \alpha)$ erit divisorum forma; sic cum casu $N = 13$ una divisorum formulae $aa - 13bb$ forma esset $52m \pm 3$, erit quoque $52m \pm 23$ forma divisorum.

ANNOTATIO 20

Sin autem fuerit N vel numerus impariter par vel numerus impar formae $4n - 1$, tum ista formarum dividentium reductio ad duplo pauciores non succedit. Scilicet si hoc casu formulae $aa - Nbb$ fuerit $4Nm \pm \alpha$ divisorum forma, tum $4Nm \pm (2N - \alpha)$ talis non erit, hoc est: Nullus numerus in forma $2(2m \pm 1)N \pm \alpha$ contentus erit divisor ullius numeri huiusmodi $aa - Nbb$. Posito ergo $\alpha = tt$ erit $(2(2m \pm 1)N \pm tt)u \mp aa - Nbb$. Unde consequimur sequens

CONSECTARIUM

Nullus numerus in hac forma $2abc \pm c + b$ contentus unquam potest esse quadratus, siquidem fuerit a numerus impar et b numerus seu impariter par seu impar huius formae $4n - 1$.

SCHOLION 2

Huiusmodi formulae magis speciales, quae nunquam quadrata fieri queant, innumerabiles superioribus deduci possunt. Consideremus enim priorem formam $aa+Nbb$ sitque $4Nm+A$ eiusmodi formula, ut nullus numerus in ea contentus possit esse divisor formae $aa+Nbb$. Erit ergo $aa+Nbb \mathrel{\Pi} (4Nm+A)u$ denotante hoc signo Π aequationem impossibilem, ex quo oritur $aa \mathrel{\Pi} 4Nmu+Au-Nbb$. Sit $b=Ac$; fiet

$$aa \mathrel{\Pi} 4Nmu+Au-NAAcc.$$

Ponatur porro $u=NAcc+d$ eritque $aa \mathrel{\Pi} 4NNAmcc+4Nmd+Ad$. Sit $d=4NNn$; erit $aa \mathrel{\Pi} 16N^3mn+4NNAmcc+4NNAn$. Dividatur haec formula per quadratum $4NN$ ac ponatur $c=1$ eritque $4Nmn+Am+An$ formula, quae nunquam poterit esse quadratum, siquidem forma $aa+Nbb$ non possit dividi per ullum numerum in hac formula $4Nm+A$ contentum. Ex superioribus ergo theorematis colligimus nullum numerum, qui in una sequentium expressionum contineatur, fieri posse quadratum:

$4mn-(m+n)$,	$4mn+3(m+n)$,
$8mn-(m+n)$,	$8mn+7(m+n)$,
$8mn-3(m+n)$,	$8mn+5(m+n)$,
$12mn-(m+n)$,	$12mn+11(m+n)$,
$12mn-7(m+n)$,	$12mn+5(m+n)$,
$20mn-(m+n)$,	$20mn+19(m+n)$,
$20mn-3(m+n)$,	$20mn+17(m+n)$,
$20mn-7(m+n)$,	$20mn+13(m+n)$,
$20mn-9(m+n)$,	$20mn+11(m+n)$,
$24mn-(m+n)$,	$24mn+23(m+n)$,
$24mn-5(m+n)$,	$24mn+19(m+n)$,
$24mn-7(m+n)$,	$24mn+17(m+n)$,

$$24mn - 11(m+n), \qquad 24mn + 13(m+n),$$
$$28mn - (m+n), \qquad 28mn + 27(m+n),$$
$$28mn - 9(m+n), \qquad 28mn + 19(m+n),$$
$$28mn - 11(m+n), \qquad 28mn + 17(m+n),$$
$$28mn - 15(m+n), \qquad 28mn + 13(m+n),$$
$$28mn - 23(m+n), \qquad 28mn + 5(m+n),$$
$$28mn - 25(m+n), \qquad 28mn + 3(m+n)$$

etc.

Notandum autem est in formulis alterius columnae numeros m et n respectu coefficientis ipsius $m+n$ primos esse oportere. Hanc restrictionem requirit ea conditio, quam initio stabilivimus, ut in forma $aa+Nbb$ numeri a et b sint inter se numeri primi; nisi enim haec conditio observetur, quilibet numerus posset esse divisor istius formae. Ceterum hac conditione observata ex praecedentibus perspicuum est, si $4Nmn - A(m+n)$ quadratum esse nequeat, tum quoque hanc latius patentem $4Nmn - A(m+n) \pm 4Np(m+n)$ quadratum esse non posse.

SCHOLION 3

Contemplemur iam expressionem $aa - Nbb$, cuius nullus divisor contineatur in formula hac $4Nm \pm A$. Erit ergo $aa - Nbb = 4Nmu \pm Au$ seu $aa = 4Nmu + NAA \pm Au$. Ponatur $NA \pm u = d$ seu $u = \pm d \mp NA$ eritque $aa = \pm 4Nmd \mp 4NNAm + Ad$. Sit $d = \pm 4NNn$ fietque

$$16N^3mn \mp 4NNAm \pm 4NNAn = aa,$$

unde patet nullum numerum contentum in hac formula $4Nmn \pm A(m-n)$ quadratum esse posse. Neque ergo etiam ullus numerus in hac expressione $4Nmn \pm A(m-n) \pm 4pN(m-n)$ contentus quadratum esse poterit, si modo conditio ante memorata observetur, ut a et b sint numeri inter se primi. Hinc itaque ex theorematis posterioribus deducuntur sequentes formulae, quae nunquam numeros quadratos praebere possunt:

$$\begin{array}{ll}
8mn \pm 3(m-n), & 8mn \pm 5(m-n), \\
12mn \pm 5(m-n), & 12mn \pm 7(m-n), \\
20mn \pm 3(m-n), & 20mn \pm 17(m-n), \\
20mn \pm 7(m-n), & 20mn \pm 13(m-n), \\
24mn \pm 7(m-n), & 24mn \pm 17(m-n), \\
24mn \pm 11(m-n), & 24mn \pm 13(m-n), \\
28mn \pm 5(m-n), & 28mn \pm 23(m-n), \\
28mn \pm 11(m-n), & 28mn \pm 17(m-n), \\
28mn \pm 13(m-n), & 28mn \pm 15(m-n)
\end{array}$$

etc.

Attendenti autem facile patebit ambos numeros m et n respectu coefficientis ipsius $(m-n)$ primos esse debere; alioquin enim, si verbi gratia in formula $12mn \pm 5(m-n)$ poneretur $m = 5p$ et $n = 5q$, prodiret $12 \cdot 25pq \pm 25(p-q)$ neque adeo haec formula $12pq \pm (p-q)$ quadratum esse posset; quod tamen est falsum.

SOLUTIO PROBLEMATIS DIFFICILLIMI A FERMATIO PROPOSITI

Commentatio 167 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 2 (1749), 1751, p. 49—67
Summarium ibidem p. 6—7

SUMMARIUM

Cum FERMATIUS proximo elapso saeculo, Galliae decus, plurimum studii et operae in problematibus ad methodum DIOPHANTI pertinentibus felicissimo successu consumsisset et haec Analyseos pars post eius tempora non eadem cura ac reliquae praedictae disciplinae partes promota, immo a Geometris, qui eum sunt secuti, fere neglecta sit, idcirco Cel. EULERUS partem hanc Analyseos, quae circa numeros est occupata et ad problemata indeterminata solvenda adhiberi solet, vel ideo colendam sibi sumsit, quoniam plerumque summa ingenii vis in talibus huius doctrinae problematibus, quae olim solutu difficilia sunt habita, cernatur atque ab Analysta non mediocris ad ea solvenda requiratur sagacitas.

Problema autem, quod sibi in hac dissertatione inveniendum sumsit Cel. EULERUS et quod a FERMATIO, qui id in annotationibus suis ad *DIOPHANTUM* BACHETI proposuerat idque solutu difficillimum iudicaverat, est sequens:

Invenire triangulum rectangulum in numeris rationalibus expressum, cuius uterque cathetus area ipsius trianguli minutus producat numerum quadratum.

Postquam igitur Cel. Auctor praeparationem ad solutionem praemisit, tres huius problematis solutiones particulares ceteris, quas elicere potuisset, omissis exhibet simulque viam monstrat, quomodo ex praeparatione ad solutiones supra traditas solutio quaedam generalis et concinna, quam in dissertatione ipsa uberius exemplis illustrat, deducta sit.

1. Quamquam problemata, quae olim solutu difficilia sunt habita, hodie plerumque ob fines Analyseos tantopere promotos nihil vel parum difficultatis habere solent, tamen hoc in eo problematum genere, quae ad methodum Diophanti pertinent, non usu venit. In hac enim Analyseos parte post Fermatii tempora, qui plurimum studii et operae in ea felicissimo cum successu consumsit, non solum nihil ultra praestitum esse videtur, sed etiam hoc studium a Geometris, qui eum sunt secuti, fere penitus est neglectum. Etsi autem ea Analyseos pars, in qua Mathematici hodie potissimum versantur, ob summam utilitatem, quam ad reliquas scientias atque artes copiosissime affert, omni laude maxime digna est habenda, tamen altera quoque pars, quae in numeris est occupata et ad problemata indeterminata solvenda adhiberi solet, idcirco minime est contemnenda, cum in ea plerumque summa ingenii vis cernatur atque ab Analysta non mediocris sagacitas requiratur.

2. Quae cum ita sint comparata, ea huius generis problemata, quae a Fermatio summopere difficilia sunt iudicata, eadem et hodie non magis facta sunt facilia hincque studium, quod in eorum solutione ponitur, non male collocatur. Proponit autem Fermatius in annotationibus suis ad *Diophantum Bacheti*[1]) sequens problema tanquam solutu difficillimum:

Invenire triangulum rectangulum in numeris rationalibus expressum, cuius uterque cathetus area ipsius trianguli minutus producat numerum quadratum.

Huius ergo problematis sequentes, quas mihi quidem elicere contigit, solutiones in medium afferre visum est.

PRAEPARATIO AD SOLUTIONEM

3. Notum est triangulum rectangulum in numeris rationalibus exprimi, si ponatur cathetorum alter $= 2ab$ et alter $= aa - bb$; tum enim prodibit hypotenusa $= aa + bb$.[2]) Generalius catheti ambo poni possunt $\frac{2ab}{z}$ et $\frac{aa-bb}{z}$ prodeunte hypotenusa $= \frac{aa+bb}{z}$. Ponam autem, quoniam naturam trianguli

1) Vide notam 2 p. 51. Problema hic tractandum invenitur in Fermatii observatione ad quaestionem XIV libri VI Diophanti, p. 302; *Oeuvres de Fermat*, t. I, p. 333. F. R.

2) Vide lemma 2 Commentationis 98, p. 39 huius voluminis. F. R.

rectanguli ultimo loco in computum vocare expedit,

$$\text{unum cathetum} = \frac{2x}{z}, \quad \text{alterum cathetum} = \frac{y}{z}$$

eritque area

$$= \frac{xy}{zz}.$$

Ac primo per conditionem problematis hae quantitates

$$\text{I.} \quad \frac{2x}{z} - \frac{xy}{zz} \quad \text{seu} \quad 2xz - xy,$$

$$\text{II.} \quad \frac{y}{z} - \frac{xy}{zz} \quad \text{seu} \quad yz - xy$$

quadrata effici debent. Tum vero, quia hypotenusa fit $= \frac{\sqrt{(4xx+yy)}}{z}$, haec quantitas

$$\text{III.} \quad 4xx + yy$$

reddi debet quadratum.

4. Quoniam hae ambae quantitates $2xz - xy$ et $yz - xy$ esse debent quadrata, earum productum pariter erit quadratum. Ordior ergo a producto

$$2xyzz - 2xxyz - xyyz + xxyy,$$

quod quadratum reddi debet, ponoque eius radicem $= xy - \frac{p}{q}yz$, ut ex evolutione valor ipsius z commode definiri queat; fiet autem

$$2xyzz - 2xxyz - xyyz + xxyy = xxyy - \frac{2p}{q}xyyz + \frac{pp}{qq}yyzz.$$

Ac deleto utrinque termino communi $xxyy$ et reliqua aequatione per yz divisa obtinebitur

$$2xz - 2xx - xy = \frac{-2p}{q}xy + \frac{pp}{qq}yz,$$

unde fit

$$z = \frac{2qqxx + qqxy - 2pqxy}{2qqx - ppy}.$$

5. Invento iam valore ipsius z fiet

$$2z - y = \frac{4qqxx - 4pqxy + ppyy}{2qqx - ppy} = \frac{(2qx - py)^2}{2qqx - ppy},$$

$$z - x = \frac{ppxy + qqxy - 2pqxy}{2qqx - ppy} = \frac{xy(p-q)^2}{2qqx - ppy}$$

hincque porro habebitur

$$2xz - xy = \frac{x(2qx - py)^2}{2qqx - ppy} = \frac{xx(2qx - py)^2}{2qqxx - ppxy},$$

$$yz - xy = \frac{xyy(p-q)^2}{2qqx - ppy} = \frac{xxyy(p-q)^2}{2qqxx - ppxy}.$$

Quarum quantitatum cum utraque esse debeat quadratum, hoc efficietur, dummodo communis denominator $2qqxx - ppxy$ fiat quadratum. Ponatur in hunc finem

$$2qqxx - ppxy = rrxx$$

ac divisione facta per x erit

$$(2qq - rr)x = ppy \quad \text{et} \quad \frac{x}{y} = \frac{pp}{2qq - rr}.$$

6. Sufficiet autem ad nostram solutionem nosse relationem inter x et y, quia in calculum iam introductus est communis denominator z; quare ponere licebit

$$x = pp \quad \text{et} \quad y = 2qq - rr,$$

unde fiet $z - x = \frac{pp(2qq - rr)(p-q)^2}{pprr}$ ideoque

$$z = pp + \frac{(2qq - rr)(p-q)^2}{rr}.$$

Ideoque superest tantum, ut $4xx + yy$ reddatur quadratum, unde sequens expressio debet esse quadratum

$$4p^4 + 4q^4 - 4qqrr + r^4,$$

unde sequentes solutiones particulares adornabuntur.

SOLUTIO PRIMA

7. Quoniam igitur quaestio huc est reducta, ut pro litteris p, q, r eiusmodi valores assignentur, qui hanc expressionem $4p^4+4q^4-4qqrr+r^4$ reddant quadratum, solutio generalis, quae omnes omnino valores idoneos harum litterarum complectatur, tradi nequit. Cum igitur solutionibus specialibus acquiescere debeamus, ponam primo radicem huius expressionis esse $=2pp\mp rr$, ut termini $4p^4$ et r^4 utrinque se destruant, ac prodibit haec aequatio

$$4q^4-4qqrr=\mp 4pprr,$$

unde fit $pp=\mp\frac{qq}{rr}(qq-rr)$, et habebimus

$$\text{vel}\quad p=\frac{q}{r}\sqrt{(qq-rr)}\quad\text{vel}\quad p=\frac{q}{r}\sqrt{(rr-qq)}.$$

8. Priori formulae $p=\frac{q}{r}\sqrt{(qq-rr)}$ satisfit ponendo $q=cc+dd$ et $r=2cd$, unde fit $p=\frac{(cc+dd)(cc-dd)}{2cd}$. Ex his ergo valoribus

$$q=cc+dd,\quad r=2cd,\quad p=\frac{(cc+dd)(cc-dd)}{2cd}$$

seu

$$p=(cc+dd)(cc-dd),\quad q=2cd(cc+dd),\quad r=4ccdd$$

erit

$$x=pp,\quad y=2qq-rr,\quad \sqrt{(4xx+yy)}=2pp+rr,\quad z=x+\frac{y(p-q)^2}{rr},$$

quibus inventis erit pro triangulo rectangulo quaesito

$$\text{I. cathetus}=\frac{2x}{z},\qquad \text{II. cathetus}=\frac{y}{z}.$$

EXEMPLUM 1

9. Sit $c=2$ et $d=1$ ac prodibunt hi valores

$$p=5\cdot 3=15,\quad q=4\cdot 5=20,\quad r=4\cdot 4=16,$$

$$x=225,\quad y=544,\quad z=225+\frac{544\cdot 25}{256}=\frac{25\cdot 89}{8}=\frac{2225}{8}$$

atque

$$\sqrt{(4xx+yy)}=2pp+rr=706,$$

ex quibus conficitur hoc triangulum rectangulum in numeris

$$\text{I. cath. } \frac{2x}{z}=\frac{144}{89}, \quad \text{II. cath. } \frac{y}{z}=\frac{4352}{25\cdot 89}, \quad \text{III. hypot.}=\frac{5648}{25\cdot 89};$$

area ergo erit $=\frac{72\cdot 4352}{25\cdot 89^2}$ et problemati ita satisfit:

$$\text{I. cath.} - \text{area} = \frac{144}{25\cdot 89^2}(25\cdot 89-2176) = \frac{144\cdot 49}{25\cdot 89^2} = \left(\frac{12\cdot 7}{5\cdot 89}\right)^2,$$

$$\text{II. cath.} - \text{area} = \frac{4352}{25\cdot 89^2}(89-72) = \frac{17\cdot 17\cdot 256}{25\cdot 89^2} = \left(\frac{16\cdot 17}{5\cdot 89}\right)^2.$$

EXEMPLUM 2

10. Sit $c=3$ et $d=1$ ac sequentes prodibunt valores

$$p=10\cdot 8, \quad q=6\cdot 10, \quad r=6\cdot 6,$$

qui per 4 divisi ad minores terminos hos reducuntur

$$p=20, \quad q=15, \quad r=9.$$

Ex his fit

$$x=400, \quad y=369 \quad \text{et} \quad z=\frac{4625}{9}, \quad \sqrt{(4xx+yy)}=881,$$

unde triangulum rectangulum erit

$$\text{I. cath. } \frac{2x}{z}=\frac{32\cdot 9}{185}, \quad \text{II. cath. } \frac{y}{z}=\frac{81\cdot 41}{25\cdot 185}, \quad \text{III. hypot.}=\frac{9\cdot 881}{25\cdot 185}$$

atque area $=\frac{16\cdot 9\cdot 81\cdot 41}{25\cdot 185^2}$; quare problemati ita satisfit:

$$\text{I. cath.} - \text{area} = \frac{2\cdot 16\cdot 9\cdot 25\cdot 185-16\cdot 9\cdot 81\cdot 41}{25\cdot 185^2} = \frac{16\cdot 9\cdot 5929}{25\cdot 185^2} = \left(\frac{4\cdot 3\cdot 77}{5\cdot 185}\right)^2,$$

$$\text{II. cath.} - \text{area} = \frac{81\cdot 41\cdot 185-16\cdot 9\cdot 81\cdot 41}{25\cdot 185^2} = \frac{81\cdot 41\cdot 41}{25\cdot 185^2} = \left(\frac{9\cdot 41}{5\cdot 185}\right)^2.$$

SOLUTIO SECUNDA

11. Sumatur ex solutione praecedente casus posterior $p=\frac{q}{r}\sqrt{(rr-qq)}$, qui requirit hos valores

$$r = cc + dd, \quad q = 2cd, \quad p = \frac{2cd(cc-dd)}{cc+dd}$$

seu

$$r = (cc+dd)^2, \quad q = 2cd(cc+dd), \quad p = 2cd(cc-dd),$$

$$x = pp, \quad y = 2qq - rr, \quad \sqrt{(4xx+yy)} = 2pp - rr \quad \text{et ut ante} \quad z = x + \frac{y(p-q)^2}{rr}.$$

Quia autem esse debet $2qq > rr$, erit $8ccdd > (cc+dd)^2$ et $2cd\sqrt{2} > cc + dd$ seu $0 > cc - 2cd\sqrt{2} + dd$, quod huc redit, ut sit $dd > (c - d\sqrt{2})^2$; ergo

$$\text{vel} \quad d > c - d\sqrt{2} \quad \text{seu} \quad \frac{d}{c} > \frac{1}{1+\sqrt{2}}$$

$$\text{vel} \quad d > d\sqrt{2} - c \quad \text{seu} \quad \frac{d}{c} < \frac{1}{\sqrt{2}-1}.$$

Ergo si $d = 1$, necesse est, ut sit vel $c < \sqrt{2} + 1$ vel $c > \sqrt{2} - 1$. At est $c > 1$, unde semper erit $c > \sqrt{2} - 1$ et $2qq - rr$ fiet quantitas positiva. Erit itaque

$$\text{I. cath.} = \frac{2x}{z}, \qquad \text{II. cath.} = \frac{y}{z} \qquad \text{et} \qquad \text{III. hypot.} = \frac{\sqrt{(4xx+yy)}}{z}.$$

EXEMPLUM 1

12. Sit $c = 2$ et $d = 1$ ac provenient hi valores

$$r = 5 \cdot 5 = 25, \quad q = 4 \cdot 5 = 20, \quad p = 4 \cdot 3 = 12$$

hincque

$$x = 144, \quad y = 175, \quad \sqrt{(4xx+yy)} = 337 \quad \text{atque} \quad z = 144 + \frac{175 \cdot 64}{625} = \frac{4048}{25}.$$

Unde trianguli quaesiti erit

$$\text{I. cath.} = \frac{2x}{z} = \frac{288 \cdot 25}{4048} = \frac{18 \cdot 25}{253} = \frac{450}{253},$$

$$\text{II. cath.} = \frac{y}{z} = \frac{25 \cdot 175}{4048} = \frac{4375}{4048},$$

$$\text{III. hypot.} = \frac{\sqrt{(4xx+yy)}}{z} = \frac{25 \cdot 337}{4048} = \frac{8425}{4048}.$$

Area itaque erit $= \frac{225 \cdot 4375}{253 \cdot 4048} = \frac{225 \cdot 4375}{16 \cdot 253^2}$, unde problemati hoc modo satisfit, ut sit:

$$\text{I. cath.} - \text{area} = \frac{225(32\cdot 253 - 4375)}{16\cdot 253^2} = \frac{225\cdot 61^2}{16\cdot 253^2} = \left(\frac{15\cdot 61}{4\cdot 253}\right)^2,$$

$$\text{II. cath.} - \text{area} = \frac{25(175\cdot 253 - 9\cdot 4375)}{253\cdot 4048} = \frac{25\cdot 25\cdot 7\cdot 28}{16\cdot 253^2} = \left(\frac{25\cdot 14}{4\cdot 253}\right)^2.$$

EXEMPLUM 2

13. Sit $c = 3$ et $d = 1$ ac prodibunt hi valores

$$r = 10\cdot 10, \quad q = 6\cdot 10, \quad p = 6\cdot 8$$

seu

$$r = 25, \quad q = 15, \quad p = 12$$

hincque

$$x = 144, \quad y = 175, \quad \sqrt{(4xx + yy)} = 337;$$

qui valores cum sint iidem qui in exemplo praecedente, hinc nulla nova oritur solutio.[1]) Maiores autem numeros pro c et d non substituo, quod inde nimis complicati valores pro x, y et z prodeunt; praecipua enim cura in hoc debet poni, ut triangula in minimis, quantum fieri potest, numeris expressa reperiantur.

SOLUTIO TERTIA

14. Cum $4xx + yy = 4p^4 + 4q^4 - 4qqrr + r^4$ esse debeat quadratum, eius radicem ponamus hic $= 2pp \pm 2qq$, ut sit $\sqrt{(4xx + yy)} = 2pp \pm 2qq$; atque prodibit haec aequatio

$$r^4 - 4qqrr = \pm 8ppqq,$$

unde fit $pp = \pm \frac{2rr(rr - 4qq)}{16qq}$ et

$$\text{vel} \quad p = \frac{r}{4q}\sqrt{(2rr - 8qq)} \quad \text{vel} \quad p = \frac{r}{4q}\sqrt{(8qq - 2rr)}.$$

Quia vero ob $y = 2qq - rr$ esse oportet $2qq > rr$, prior valor erit inutilis habebimusque

$$p = \frac{r}{4q}\sqrt{(8qq - 2rr)}, \quad x = pp, \quad y = 2qq - rr \quad \text{et} \quad \sqrt{(4xx + yy)} = 2pp - 2qq$$

1) Revera est $y = -175$. Ob valorem negativum ipsius y hoc exemplum reiici debet. F. R.

atque ut ante $z = x + \frac{y(p-q)^2}{rr}$. Erit ergo

$$\text{I. cath.} = \frac{2x}{z}, \quad \text{II. cath.} = \frac{y}{z}, \quad \text{III. hypot.} = \frac{\sqrt{(4xx+yy)}}{z}.$$

Nunc ergo huc devenimus, ut $8qq - 2rr$ reddatur quadratum. Sit eius radix $= \frac{c}{d}(2q+r)$ eritque $4q - 2r = \frac{cc}{dd}(2q+r)$ seu $4ddq - 2ddr = 2ccq + ccr$ hincque $q = cc + 2dd$ et $r = 4dd - 2cc$, $2q + r = 8dd$ atque $\sqrt{(8qq - 2rr)} = 8cd$ hincque $p = \frac{4cd(2dd-cc)}{2dd+cc}$. Quare in integris multiplicando per $2dd + cc$ fiet

$$p = 4cd(2dd - cc), \quad q = (2dd+cc)^2, \quad r = 2(2dd-cc)(2dd+cc),$$

$$x = pp, \quad y = 2qq - rr, \quad \sqrt{(4xx+yy)} = 2pp - 2qq, \quad z = x + \frac{y(p-q)^2}{rr}.$$

EXEMPLUM 1

15. Sit $c = 1$, $d = 1$; erit

$$p = 4, \quad q = 9, \quad r = 6,$$

$$x = 16, \quad y = 126, \quad \sqrt{(4xx+yy)} = 130 \quad \text{et} \quad z = 16 + \frac{126 \cdot 25}{36} = \frac{207}{2} = \frac{9 \cdot 23}{2},$$

$$\text{I. cath.} = \frac{64}{207}, \quad \text{II. cath.} = \frac{252}{207}, \quad \text{III. hypot.} = \frac{260}{207}.$$

Area vero erit $= \frac{64 \cdot 126}{207 \cdot 207} = \frac{64 \cdot 14}{9 \cdot 23^2}$ sicque fiet:

$$\text{I. cath.} - \text{area} = \frac{64}{9 \cdot 23^2}(23 - 14) = \frac{64}{23^2} = \left(\frac{8}{23}\right)^2,$$

$$\text{II. cath.} - \text{area} = \frac{252 \cdot 23 - 64 \cdot 14}{9 \cdot 23^2} = \frac{28 \cdot 175}{9 \cdot 23^2} = \frac{4 \cdot 7^2 \cdot 5^2}{9 \cdot 23^2} = \left(\frac{2 \cdot 5 \cdot 7}{3 \cdot 23}\right)^2.$$

Hocque exemplum sine dubio in numeris minimis existit, uti deinceps [§ 30] ostendam.

EXEMPLUM 2

16. Quia debet esse $2qq > rr$, oportet, ut sit $\frac{c}{d} > 2 - \sqrt{2}$; nihilque refert, sive sit $2dd > cc$ sive minus, quia nihil obstat, quominus p, q, r esse queant numeri negativi.

Sit igitur $d = 2$, $c = 3$; erit $2dd - cc = -1$, $2dd + cc = 17$ atque

$$p = -24 \cdot 1 = -24, \quad q = 17\ \ 17 = 289, \quad r = -2 \cdot 17 = -34,$$

$$x = 576, \quad y = 2 \cdot 7 \cdot 41 \cdot 17^2, \quad \sqrt{(4xx + yy)} = 2 \cdot 5 \cdot 53 \cdot 313,$$

$$z = 576 + \frac{2 \cdot 7 \cdot 41 \cdot 17^2 \cdot 313^2}{34^2} = \frac{28118255}{2}.\text{[1]}$$

$$\text{I. cath.} = \frac{2304}{28118255}, \quad \text{II. cath.} = \frac{28 \cdot 41 \cdot 17^2}{28118255}, \quad \text{III. hypot.} = \frac{4 \cdot 5 \cdot 53 \cdot 313}{28118255}.$$

17. In his omnibus exemplis notari meretur perinde esse, sive litterarum c et d valores capiantur affirmativi sive negativi; inde enim tantum valores p vel q vel r prodeunt negativi neque propterea valores x et y alterantur. Verum valor psius z variationem subit, ex quo pro z semper duplex valor assignari poterit, lter, qui iam est exhibitus $z = x + \frac{y(p-q)^2}{rr}$, alter vero $z = x + \frac{y(p+q)^2}{rr}$; icque ob duplicem valorem ipsius z singula exempla allata duplicabuntur.

18. Huiusmodi solutiones particulares plures adhuc elicere licet, dum liae idoneae quantitates pro radice quadrata huius formae $4p^4 + 4q^4 - 4qqrr + r^4$ ssumuntur. Veluti si haec radix ponitur $rr + 2qq \pm 2pp$, obtinebitur haec equatio

$$-4qqrr = 4qqrr \pm 4pp(2qq + rr) \quad \text{seu} \quad pp(2qq + rr) = \mp 2qqrr,$$

nde patet signum inferius valere esseque

$$\sqrt{(4xx + yy)} = rr + 2qq - 2pp$$

xistente

$$\text{vel} \quad p = \frac{2qr}{\sqrt{2(2qq + rr)}} \quad \text{vel} \quad q = \frac{pr}{\sqrt{2(rr - pp)}},$$

1) Editio princeps nec non *Commentationes arithmeticae*: $z = \frac{90983}{2}$, I. *cath.* $= \frac{2304}{90983}, \ldots$ lsus numerator ipsius z ex formula manca

$$z = 576 + \frac{2 \cdot 7 \cdot 41 \cdot 17^2 \cdot 313}{34^2}$$

tus est. Correxit F. R.

quae formulae iam facile rationales redduntur. Hic ergo si ponatur $r=3$, $p=1$, erit $q=\frac{3}{4}$ et in integris

$$p=4, \quad q=3, \quad r=12,$$

$$x=16, \quad y=-126, \quad \sqrt{(4xx+yy)}=130,$$

qui casus ob y negativum non convenit quaestioni.

19. Quoniam cardo quaestionis in hoc versatur, ut haec expressio reddatur quadratum $4p^4+(2qq-rr)^2$, potest hoc generaliter ita effici, ut eius radix ponatur $=2qq-rr+\frac{2m}{n}pp$, unde fiet $pp=\frac{m}{n}(2qq-rr)+\frac{mm}{nn}pp$ seu $(nn-mm)pp=mn(2qq-rr)$ et

$$p=\sqrt{\frac{mn(2qq-rr)}{nn-mm}}=mn\sqrt{\frac{2qq-rr}{mn(nn-mm)}},$$

cui conditioni satisfiet eiusmodi numeros pro m et n quaerendo, ut sit $mn(nn-mm)$ numerus huius formae $2ff-gg$. Verum haec solutio facilius obtinetur ex ipsa praeparatione ad solutionem tradita, quae, si recte tractetur, omnes solutiones non solum in se complectitur, sed etiam solutiones in minoribus numeris omnes commode exhibet. Eam data opera evolvam.

SOLUTIO GENERALIS

20. Assumtis cathetis trianguli quaesiti $\frac{2x}{z}$ et $\frac{y}{z}$ ponatur statim, ut anguli recti ratio habeatur, $x=ab$, $y=aa-bb$ eritque trianguli

$$\text{I. cath.}=\frac{2ab}{z}, \quad \text{II. cath.}=\frac{aa-bb}{z}, \quad \text{III. hypot.}=\frac{aa+bb}{z}$$

et area huius trianguli erit $=\frac{ab(aa-bb)}{zz}$.

Invenimus autem primo (§ 4)

$$z=\frac{2qqxx+qqxy-2pqxy}{2qqx-ppy} \quad \text{seu} \quad z=x+\frac{xy(p-q)^2}{2qqx-ppy};$$

vel quia q tam negative quam affirmative accipere licet, erit

$$z = x + \frac{xy(p \pm q)^2}{2qqx - ppy}$$

existente $x = ab$ et $y = aa - bb$.

21. Tum vero (§ 5) hanc quantitatum x et y indolem invenimus, ut sit $2qqxx - ppxy = rrxx$, unde fit

$$z = x + \frac{y(p \pm q)^2}{rr} = ab + \frac{(aa - bb)(p \pm q)^2}{rr}.$$

Nihil aliud ergo efficiendum restat, nisi ut haec aequatio $2qqxx - ppxy = rrxx$ seu haec

$$xy = \frac{xx}{pp}(2qq - rr)$$

conficiatur; ubi cum sit $xy = ab(aa - bb)$, eiusmodi numeros pro a et b investigari oportet, ut fiat $ab(aa - bb)$ numerus huius formae $2ff - gg$ seu $(2ff - gg)hh$.

22. Ponamus igitur pro a et b iam huiusmodi valores esse erutos, ut sit

$$ab(aa - bb) = (2ff - gg)hh.$$

Cum igitur ob $x = ab$ sit

$$(2ff - gg)hh = \frac{aabb}{pp}(2qq - rr),$$

hinc statim sponte se prodit

$$\frac{abq}{p} = fh \quad \text{et} \quad \frac{abr}{p} = gh.$$

Sit ergo $p = ab$; erit $q = fh$ et $r = gh$ atque

$$z = ab + \frac{(aa - bb)(ab \pm fh)^2}{gghh}$$

eruntque trianguli rectanguli quaesiti latera

$$\text{I. cath.} = \frac{2ab}{z} = \frac{2abgghh}{abgghh+(aa-bb)(ab\pm fh)^2}\ ^{1)},$$

$$\text{II. cath.} = \frac{aa-bb}{z} = \frac{(aa-bb)gghh}{abgghh+(aa-bb)(ab\pm fh)^2}\ ^{1)},$$

$$\text{III. hypot.} = \frac{aa+bb}{z} = \frac{(aa+bb)gghh}{abgghh+(aa-bb)(ab\pm fh)^2}\ ^{1)}.$$

23. Possunt etiam ex huiusmodi valoribus ipsarum a et b quibusvis innumerabilia triangula rectangula, quae quaesito satisfaciant, erui. Posito enim $p = ab$ si sit $ab(aa-bb) = (2ff-gg)hh$, erit

$$(2ff-gg)hh = 2qq - rr \quad \text{seu} \quad 2(ffhh - qq) = gghh - rr.$$

Ponatur $2(fh+q) = \frac{m}{n}(gh+r)$ eritque $fh - q = \frac{n}{m}(gh-r)$ et hinc reperietur

$$q = \frac{2mngh-(2nn+mm)fh}{2nn-mm}, \qquad r = \frac{(2nn+mm)gh-4mnfh}{2nn-mm};$$

vel in numeris integris erit

$$p = (2nn-mm)ab,$$

$$q = 2mngh - (2nn+mm)fh,$$

$$r = (2nn+mm)gh - 4mnfh.$$

24. Inventis sic valoribus his p, q et r erit

$$z = \frac{abrr+(aa-bb)(p\pm q)^2}{rr}$$

atque trianguli quaesiti latera erunt

$$\text{I. cath.} = \frac{2ab}{z}, \quad \text{II. cath.} = \frac{aa-bb}{z} \quad \text{et} \quad \text{III. hypot.} = \frac{aa+bb}{z},$$

1) Editio princeps atque etiam *Comment. arithm.* denominatorem exhibent

$$2abgghh+(aa-bb)(ab\pm fh)^2.$$ Correxit F. R.

unde pro singulis idoneis valoribus ipsarum a et b, ut sit $ab(aa-bb)=(2ff-gg)hh$, ob m et n numeros pro arbitrio assumendos innumerabilia triangula exhiberi poterunt.

25. Quoniam igitur totum negotium huc redit, ut pro a et b eiusmodi numeri assumantur, ut productum $ab(aa-bb)$ sive $ab(a+b)(a-b)$ fiat numerus huius formae $(2ff-gg)hh$, quo hoc facilius effici possit, indolem numerorum, qui in hac forma generali $(2ff-gg)hh$ seu hac $2tt-uu$ continentur, attentius considerari conveniet. Ac primo quidem perspicuum est in forma $2tt-uu$ contineri omnes numeros quadratos, quippe qui prodeunt, si $u=t$; tum vero etiam in hac forma continentur omnes numeri quadrati duplicati ponendo $u=0$. Praeterea vero infiniti alii occurrunt numeri, qui usque ad 200 sunt sequentes:

1, 2, 4, 7, 8, 9, 14, 16, 17, 18, 23, 25, 28, 31, 32, 34, 36, 41, 46, 47, 49, 50, 56, 62, 63, 64, 68, 71, 72, 73, 79, 81, 82, 89, 92, 94, 97, 98, 100, 103, 112, 113, 119, 121, 124, 126, 127, 128, 136, 137, 142, 144, 146, 151, 153, 158, 161, 162, 164, 167, 169, 175, 178, 184, 188, 191, 193, 194, 196, 199, 200.

26. Si numeri primi considerentur, qui occurrunt, ii non solum omnes in hac forma $8m\pm1$ continentur, sed etiam vicissim omnes numeri primi in hac gemina forma $8m\pm1$ contenti ibi occurrunt ideoque in forma $2tt-uu$ comprehenduntur. Praeterea vero horum numerorum primorum dupla adsunt, item eorum producta tam per quosvis numeros quadratos quam per se ipsos nec non horum productorum dupla. Qua proprietate animadversa non difficile erit hos numeros, quousque libuerit, continuare.

27. Hinc porro colligitur numeros non primos in forma $2tt-uu$ contentos alios divisores, qui quidem inter se sint primi, non admittere, nisi qui ipsi sint numeri in eadem forma $2tt-uu$ contenti. Quare cum productum $ab(a+b)(a-b)$ esse debeat numerus formae $2tt-uu$ hique factores a, b, $a+b$, $a-b$ sint vel primi inter se vel ad summum binarium pro communi divisore habeant, qui ipse in forma $2tt-uu$ continetur, necesse est, ut hi singuli factores a, b, $a+b$, $a-b$ sint numeri eiusdem formae $2tt-uu$. Quo cognito ex tabula tradita non erit difficile idoneos valores pro a et b excerpere, ut non solum a et b, sed etiam $a+b$ et $a-b$ in eadem tabula existant.

28. Quodsi autem a, b et $a+b$, $a-b$ singuli sint numeri formae $2tt-uu$, tum quoque eorum productum $ab(a+b)(a-b)$ in eadem forma continebitur, quod generatim ita ostendi potest. Sint propositi duo numeri huius formae, velut $2\alpha\alpha-\beta\beta$ et $2\gamma\gamma-\delta\delta$; erit eorum productum

$$\begin{aligned}&(2\alpha\alpha-\beta\beta)(2\gamma\gamma-\delta\delta)\\ &=(2\alpha\gamma+\beta\delta)^2-2(\beta\gamma+\alpha\delta)^2\\ &=2(2\alpha\gamma+\beta\gamma+\alpha\delta+\beta\delta)^2-(2\alpha\gamma+2\beta\gamma+2\alpha\delta+\beta\delta)^2.\end{aligned}$$

Est enim generaliter

$$xx-2yy=2(x+y)^2-(x+2y)^2,$$

ita ut hae duae formae $2tt-uu$ et $tt-2uu$ inter se congruant. Cum igitur productum ex duobus numeris formae $2tt-uu$ facile ad eandem formam revocetur, etiamsi quotcunque numeri huius formae in se invicem multiplicentur, eorum productum in eadem forma comprehendi reperietur.

29. Tribuatur ergo primo ipsi b valor quidam ex tabula numerorum allata (§ 25) et in eadem tabula facile dispicietur, utrum insint tres numeri $a-b$, a, $a+b$, qui differant illo numero b. Verum hanc tabulam inspicienti mox patet pro b vel numeros impares vel per 8 divisibiles tantum assumi posse, siquidem a et b numeri debent esse inter se primi. Huiusmodi igitur valoribus pro b substitutis pro a sequentes prodibunt valores:

b	valores ipsius a
1	8, 17, 63, 72, 127
7	9, 16, 25, 144
8	9, 17, 71, 81, 89, 161
9	16, 23, 25, 32, 41, 73, 103, 112, 128, 137, 184
16	25, 47, 63, 97, 137, 153
17	64, 81, 144, 161
23	41, 121, 144
25	56, 72, 119, 128, 137, 144, 153, 169

b	valores ipsius a
31	32, 63, 72, 81, 113, 144
32	41, 49, 81, 121
41	72, 103, 112, 153
47	56, 72, 79, 81, 97, 128, 144
49	72, 113[1])
56	81, 97, 137
63	64, 79, 136
64[2])	73, 89, 127
71	73
72	79, 89, 97, 103, 119, 121
74	89
79	—
81	97, 112, 113.

EXEMPLUM 1

30. Quo usus huius tabulae ad solutionem problematis clarius appareat, sit $b=1$, $a=8$ eritque

$$ab=8, \quad aa-bb=63, \quad ab(aa-bb)=8\cdot 9\cdot 7=4\cdot 9\cdot 14.$$

Fiet ergo $4\cdot 9\cdot 14=hh(2ff-gg)$ ideoque $h=6$ et $2ff-gg=14$, unde colligitur $f=3$, $g=2$; et ex § 23 obtinebimus

$$p=8(2nn-mm), \quad q=24mn-18(2nn+mm), \quad r=12(2nn+mm)-72mn,$$

qui sublato communi divisore 2 erunt

1) In editione principe atque etiam in *Comment. arithm.* hic sequitur numerus 146, qui autem non est idoneus. F. R.

2) In editione principe atque etiam in *Comment. arithm.* tota haec series deest. F. R.

$$p = 8nn - 4mm, \quad q = 12mn - 18nn - 9mm, \quad r = 12nn + 6mm - 36mn,$$

$$p + q = 12mn - 10nn - 13mm, \quad -p + q = 12mn - 26nn - 5mm$$

et

$$z = 8 + \frac{63(p \pm q)^2}{rr}.$$

Hinc ergo innumerabiles prodeunt valores ipsius z, ex quorum quovis conficitur triangulum rectangulum

$$\text{I. cath.} = \frac{16}{z}, \quad \text{II. cath.} = \frac{63}{z}, \quad \text{III. hypot.} = \frac{65}{z}.$$

Casusque omnium simplicissimus oritur ponendo $n = 0$ et $m = 1$, unde fit $r = 6$, $p \pm q = \begin{cases} 5 \\ 13 \end{cases}$ et $z = 8 + \frac{7}{4} \cdot \begin{cases} 25 \\ 169 \end{cases}$, ergo vel $z = \frac{207}{4}$ vel $z = \frac{1215}{4}$, quorum valorum prior est pro casu simplicissimo iam § 15 exposito.

EXEMPLUM 2

31. Cum pro quibusque valoribus litterarum a et b infiniti exhiberi possint valores idonei ipsius z, quorum inventio nulla difficultate laborat per ea, quae § 23 et 24 sunt tradita, hic tantum valorem § 22 datum $z = ab + \frac{(aa - bb)(ab \pm fh)^2}{gghh}$ adhibere sufficiet ob $ab(aa - bb) = (2ff - gg)hh$; unde erunt trianguli catheti I. $= \frac{2ab}{z}$, II. $= \frac{aa - bb}{z}$ et hypot. $= \frac{aa + bb}{z}$.

Sit igitur $b = 7$ et $a = 9$; erit

$$ab = 63, \quad aa - bb = 32 \quad \text{et} \quad ab(aa - bb) = 63 \cdot 32 = 16 \cdot 9 \cdot 14 = (2ff - gg)hh,$$

unde fiet $h = 12$, $f = 3$ et $g = 2$, ergo $z = 63 + \frac{32(63 \pm 36)^2}{24 \cdot 24}$ seu $z = 63 + \frac{9(7 \pm 4)^2}{2}$ ideoque vel $z = \frac{207}{2}$ vel $z = \frac{1215}{2}$; consequenter triangulum quaesitum erit ut ante

$$\text{I. cath.} = \frac{126}{207}, \quad \text{II. cath.} = \frac{64}{207}, \quad \text{III. hypot.} = \frac{260}{207}.$$

EXEMPLUM 3

32. Quo usus tabulae § 29 exhibitae clarius perspiciatur, sumamus pro a et b maiores numeros sitque $b = 41$ et $a = 112$, ut sit $ab = 7 \cdot 16 \cdot 41$, $aa - bb = 71 \cdot 9 \cdot 17$; erit $ab(aa - bb) = 16 \cdot 9 \cdot 7 \cdot 17 \cdot 41 \cdot 71 = (2ff - gg)hh$ et $h = 12$ atque $7 \cdot 17 \cdot 41 \cdot 71 = 2ff - gg$. At est

$$7 = 3^2 - 2 \cdot 1^2, \quad 17 = 2 \cdot 3^2 - 1^2, \quad 41 = 7^2 - 2 \cdot 2^2, \quad 71 = 2 \cdot 6^2 - 1^2,$$

unde fit

$$7 \cdot 41 = (21 \pm 2 \cdot 2)^2 - 2(6 \pm 7)^2 = 17^2 - 2 \cdot 1^2 = 2 \cdot 16^2 - 15^2.$$

Atque

$$17 \cdot 71 = (2 \cdot 18 \pm 1)^2 - 2(6 \pm 3)^2 = 35^2 - 2 \cdot 3^2 = 2 \cdot 32^2 - 29^2,$$

ergo

$$7 \cdot 17 \cdot 41 \cdot 71 = (17 \cdot 35 - 2 \cdot 3)^2 - 2(51 - 35)^2 = 589^2 - 2 \cdot 16^2;$$

$$7 \cdot 17 \cdot 41 \cdot 71 = 2 \cdot 573^2 - 557^2.$$

Haec autem reductio ad formam $2tt - uu$ infinitis aliis modis fieri potest, quorum simplicissimus est hic $7 \cdot 17 \cdot 41 \cdot 71 = 2 \cdot 417^2 - 37^2$, ut sit $f = 417$ et $g = 37$. Ergo ob $h = 12$ erit $fh = 12 \cdot 3 \cdot 139$ et $gh = 12 \cdot 37$ ideoque

$$z = 16 \cdot 7 \cdot 41 + \frac{9 \cdot 17 \cdot 71(16 \cdot 7 \cdot 41 \pm 4 \cdot 9 \cdot 139)^2}{16 \cdot 9 \cdot 37 \cdot 37}$$

seu

$$z = 16 \cdot 7 \cdot 41 + \frac{17 \cdot 71(4 \cdot 7 \cdot 41 - 9 \cdot 139)^2}{37 \cdot 37}$$

vel

$$z = 16 \cdot 7 \cdot 41 + \frac{17 \cdot 71 \cdot 103 \cdot 103}{37 \cdot 37} = \frac{1909 \cdot 1511}{1369}.$$

Ex quo obtinebitur triangulum rectangulum

I. cath. $= \dfrac{9184 \cdot 1369}{19091511}$, II. cath. $= \dfrac{10863 \cdot 1369}{19091511}$, III. hypot. $= \dfrac{14225 \cdot 1369}{19091511}$.

DECOUVERTE D'UNE LOI TOUT EXTRAORDINAIRE DES NOMBRES PAR RAPPORT A LA SOMME DE LEURS DIVISEURS[1)]

Commentatio 175 indicis ENESTROEMIANI
Bibliothèque impartiale **3**, 1751, p. 10—31

1. Les Mathematiciens ont taché jusqu'ici en vain à découvrir quelque ordre dans la progression des nombres premiers, et on a lieu de croire que c'est un mystére auquel l'esprit humain ne sauroit jamais pénétrer. Pour s'en convaincre, on n'a qu'à jetter les yeux sur les tables des nombres premiers, que quelques-uns se sont donné la peine de continuer au-delà de cent mille et on s'appercevra d'abord qu'il n'y regne aucun ordre ni régle. Cette circonstance est d'autant plus surprenante, que l'Arithmetique nous fournit des régles sures, par le moyen desquelles on est en état de continuer la progression de ces nombres aussi loin qu'on souhaite, sans pourtant nous y laisser la moindre marque de quelque ordre. Je me crois aussi bien éloigné de ce but, mais je viens de découvrir une loi fort bizarre parmi les sommes des diviseurs des nombres naturels, qui, au premier coup d'oeil, paroissent aussi irrégulieres que la progression des nombres premiers, et qui semblent même enveloper celle-ci. Cette régle, que je vai expliquer, est à mon avis

1) Ce mémoire a été également publié, comme „ineditum", d'après un manuscrit de l'Académie de Berlin dans les *Commentationes arithmeticae* **2**, 1849, p. 639, et ensuite dans les *Opera postuma* **1**, 1862, p. 76, les éditeurs, P. H. et N. FUSS, n'ayant pas eu connaissance de la publication antérieure, faite dans la Bibliothèque impartiale. Cf. *Comment. arithm.* Prooemium, p. XVIII, No. 57, Suppl. Prooem., No. 1, et t. II, p. VIII; en outre P. STÄCKEL und W. AHRENS, *Der Briefwechsel zwischen C. G. J. JACOBI und P. H. VON FUSS über die Herausgabe der Werke LEONHARD EULERS*, Leipzig 1908, p. 59 et 83. Il faut remarquer que le texte de la Bibliothèque impartiale diffère sur plusieurs points de celui des *Comment. arithm.* et des *Op. post.* Nous avons reproduit intégralement dans notre édition le texte de la Bibliothèque impartiale. Voir aussi le mémoire 243 de ce volume. F. R.

d'autant plus importante qu'elle appartient à ce genre dont nous pouvons nous assurer de la vérité, sans en donner une démonstration parfaite. Néanmoins, j'en apporterai de telles preuves, qu'on pourra presque les envisager comme équivalentes à une démonstration rigoureuse.

2. Les nombres premiers se distinguent des autres nombres en ce qu'ils n'admettent d'autres diviseurs que l'unité et eux-mêmes. Ainsi 7 est un nombre premier, parce qu'il n'est divisible que par l'unité et lui-même. Les autres nombres qui ont, outre l'unité et eux-mêmes, encore d'autres diviseurs, sont nommés composés, comme par exemple le nombre 15 qui, outre l'unité et lui-même, est divisible par 3 et 5. Donc en général, si le nombre p est premier, il ne sera divisible que par 1 et par p; mais si p est un nombre composé, il aura, outre 1 et p, encore d'autres diviseurs; et partant, dans le premier cas, la somme des diviseurs sera $= 1 + p$, et dans l'autre cas, elle sera plus grande que $1 + p$. Comme mes réflexions suivantes rouleront sur la somme des diviseurs de chaque nombre, je me servirai d'un certain caractere pour la marquer. La lettre $\int$ qu'on emploie dans l'analyse des infinis pour indiquer les intégrales, étant mise devant un nombre, me marquera la somme de ses diviseurs[1]): ainsi $\int 12$ signifiera la somme de tous les diviseurs du nombre 12 qui sont $1 + 2 + 3 + 4 + 6 + 12 = 28$, de sorte que $\int 12 = 28$. Cela posé, on verra que $\int 60 = 168$ et $\int 100 = 217$. Mais, comme l'unité n'a d'autre diviseur qu'elle-même, on aura $\int 1 = 1$. Or la cyphre 0, étant divisible par tout nombre, la valeur de $\int 0$ sera infinie. Cependant, dans la suite, je lui assignerai, pour chaque cas proposé, une valeur déterminée, convenable à mon dessein.

3. Ayant donc établi ce signe $\int$ pour marquer la somme des diviseurs du nombre devant lequel il est posé, il est clair que si p marque un nombre premier, la valeur de $\int p$ sera $= 1 + p$; excepté le cas où $p = 1$, dans lequel il y a $\int 1 = 1$, et non pas $\int 1 = 1 + 1$; d'où l'on voit qu'on doit exclure l'unité de la suite des nombres premiers, de sorte que l'unité étant le com-

1) Voir les mémoires 152, 243 et surtout le mémoire 244 de ce volume. Voir aussi la lettre d'EULER à GOLDBACH du 1er avr. 1747, *Correspondance math. et phys. publiée par P. H. Fuss*, St.-Pétersbourg 1843, t. I, p. 407, et la lettre d'EULER à D'ALEMBERT du 15 février 1748 publiée par P. STÄCKEL, Biblioth. Mathem. 11_3, 1910/1, p. 220; *LEONHARDI EULERI Opera omnia*, series III. F. R.

mencement des nombres entiers, n'est ni premier ni composé. Or, si le nombre p n'est pas premier, la valeur de $\int p$ sera plus grande que $1+p$. Dans ce cas, on trouvera aisément la valeur de $\int p$ par les facteurs du nombre p. Car soient a, b, c, d, etc. des nombres premiers differens entre eux, on verra aisément que

$$\int ab = 1 + a + b + ab = (1+a)(1+b) = \int a \cdot \int b,$$
$$\int abc = (1+a)(1+b)(1+c) = \int a \cdot \int b \cdot \int c,$$
$$\int abcd = \int a \cdot \int b \cdot \int c \cdot \int d,$$
etc.

Pour les puissances des nombres premiers, on a besoin des régles particulieres, comme

$$\int a^2 = 1 + a + a^2 = \frac{a^3-1}{a-1},$$
$$\int a^3 = 1 + a + a^2 + a^3 = \frac{a^4-1}{a-1},$$

et généralement

$$\int a^n = \frac{a^{n+1}-1}{a-1}.$$

Et par le moyen de celles-ci, on pourra assigner la somme des diviseurs de chaque nombre, tout composé qu'il puisse être; ce qui sera clair par les formules suivantes:

$$\int a^2 b = \int a^2 \cdot \int b,$$
$$\int a^3 b^2 = \int a^3 \cdot \int b^2,$$
$$\int a^3 b^4 c = \int a^3 \cdot \int b^4 \cdot \int c,$$

et généralement

$$\int a^\alpha b^\beta c^\gamma d^\delta e^\varepsilon = \int a^\alpha \cdot \int b^\beta \cdot \int c^\gamma \cdot \int d^\delta \cdot \int e^\varepsilon.$$

Ainsi, pour trouver la valeur de $\int 360$, puisque 360 se résout dans ces facteurs $2^3 \cdot 3^2 \cdot 5$, j'aurai

$$\int 360 = \int 2^3 \cdot 3^2 \cdot 5 = \int 2^3 \cdot \int 3^2 \cdot \int 5 = 15 \cdot 13 \cdot 6 = 1170.$$

4. Pour mettre devant les yeux la progression des sommes des diviseurs, j'ajouterai la table suivante qui contient les sommes des diviseurs des nombres naturels depuis l'unité jusqu'à 100:

$\int 1 = 1$	$\int 21 = 32$	$\int 41 = 42$	$\int 61 = 62$	$\int 81 = 121$
$\int 2 = 3$	$\int 22 = 36$	$\int 42 = 96$	$\int 62 = 96$	$\int 82 = 126$
$\int 3 = 4$	$\int 23 = 24$	$\int 43 = 44$	$\int 63 = 104$	$\int 83 = 84$
$\int 4 = 7$	$\int 24 = 60$	$\int 44 = 84$	$\int 64 = 127$	$\int 84 = 224$
$\int 5 = 6$	$\int 25 = 31$	$\int 45 = 78$	$\int 65 = 84$	$\int 85 = 108$
$\int 6 = 12$	$\int 26 = 42$	$\int 46 = 72$	$\int 66 = 144$	$\int 86 = 132$
$\int 7 = 8$	$\int 27 = 40$	$\int 47 = 48$	$\int 67 = 68$	$\int 87 = 120$
$\int 8 = 15$	$\int 28 = 56$	$\int 48 = 124$	$\int 68 = 126$	$\int 88 = 180$
$\int 9 = 13$	$\int 29 = 30$	$\int 49 = 57$	$\int 69 = 96$	$\int 89 = 90$
$\int 10 = 18$	$\int 30 = 72$	$\int 50 = 93$	$\int 70 = 144$	$\int 90 = 234$
$\int 11 = 12$	$\int 31 = 32$	$\int 51 = 72$	$\int 71 = 72$	$\int 91 = 112$
$\int 12 = 28$	$\int 32 = 63$	$\int 52 = 98$	$\int 72 = 195$	$\int 92 = 168$
$\int 13 = 14$	$\int 33 = 48$	$\int 53 = 54$	$\int 73 = 74$	$\int 93 = 128$
$\int 14 = 24$	$\int 34 = 54$	$\int 54 = 120$	$\int 74 = 114$	$\int 94 = 144$
$\int 15 = 24$	$\int 35 = 48$	$\int 55 = 72$	$\int 75 = 124$	$\int 95 = 120$
$\int 16 = 31$	$\int 36 = 91$	$\int 56 = 120$	$\int 76 = 140$	$\int 96 = 252$
$\int 17 = 18$	$\int 37 = 38$	$\int 57 = 80$	$\int 77 = 96$	$\int 97 = 98$
$\int 18 = 39$	$\int 38 = 60$	$\int 58 = 90$	$\int 78 = 168$	$\int 98 = 171$
$\int 19 = 20$	$\int 39 = 56$	$\int 59 = 60$	$\int 79 = 80$	$\int 99 = 156$
$\int 20 = 42$	$\int 40 = 90$	$\int 60 = 168$	$\int 80 = 186$	$\int 100 = 217.$

Je ne doute pas que, pour peu qu'on regarde la progression de ces nombres, on ne désespere presque d'y découvrir le moindre ordre, vu que l'irrégularité de la suite des nombres premiers s'y trouve entremêlée tellement, qu'il semblera d'abord impossible d'indiquer quelque loi que ces nombres observent

entre eux, sans qu'on sache celle des nombres premiers. Il semble même qu'il y a ici beaucoup plus de bizarrerie que dans les nombres premiers.

5. Néanmoins, j'ai remarqué[1]) que cette progression suit une loi bien réglée et qu'elle est même comprise dans l'ordre des progressions que les Geometres nomment *recurrentes*, de sorte qu'on peut toujours former chacun de ces termes par quelques-uns des précédens, suivant une régle constante. Car si $\int n$ marque un terme quelconque de cette irréguliere progression, et $\int(n-1)$, $\int(n-2)$, $\int(n-3)$, $\int(n-4)$, $\int(n-5)$, etc. des termes précédens, je dis que la valeur de $\int n$ est toujours composée de quelques-uns des précédens suivant cette formule:

$$\begin{aligned}\int n = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \int(n-15)\\ - \int(n-22) - \int(n-26) + \int(n-35) + \int(n-40) - \int(n-51) - \int(n-57)\\ + \int(n-70) + \int(n-77) - \int(n-92) - \int(n-100) + \text{etc.}\end{aligned}$$

Dans cette formule, il y a à remarquer:

I. Que dans l'altération des signes + et —, chacun se trouve toujours mis deux fois de suite.

II. La progression des nombres 1, 2, 5, 7, 12, 15, etc. qu'il faut successivement retrancher du nombre proposé n, deviendra évidente, en prenant leurs differences:

N.	1,	2,	5,	7,	12,	15,	22,	26,	35,	40,	51,	57,	70,	77,	92,	100, etc.
Diff.	1,	3,	2,	5,	3,	7,	4,	9,	5,	11,	6,	13,	7,	15,	8,	etc.

Car alternativement, on aura tous les nombres naturels 1, 2, 3, 4, 5, 6, etc. et les nombres impairs 3, 5, 7, 9, 11, etc., d'où l'on pourra continuer la suite de ces nombres aussi loin qu'on voudra.

III. Quoique cette suite aille à l'infini, on n'en doit prendre, dans chaque cas, que les termes depuis le commencement où le nombre mis après le signe $\int$ est encore positif, en omettant ceux qui renferment des nombres négatifs.

IV. S'il arrive que le terme $\int 0$ se rencontre dans cette formule, comme sa valeur est indéterminée en elle-même, il faut, dans chaque cas, au lieu de $\int 0$, mettre le nombre même proposé.

1) Voir la lettre d'EULER à GOLDBACH citée p. 242. F. R.

6. Ces choses remarquées, il ne sera pas difficile de faire l'application de cette formule à chaque nombre proposé et de se convaincre de sa vérité, par autant d'exemples qu'on voudra déveloper. Et comme je dois avouër que je ne suis pas en état d'en donner une démonstration rigoureuse, j'en ferai voir sa justesse par un assez grand nombre d'exemples:

$$\int 1 = \int 0 = 1,$$
$$\int 2 = \int 1 + \int 0 = 1 + 2 = 3,$$
$$\int 3 = \int 2 + \int 1 = 3 + 1 = 4,$$
$$\int 4 = \int 3 + \int 2 = 4 + 3 = 7,$$
$$\int 5 = \int 4 + \int 3 - \int 0 = 7 + 4 - 5 = 6,$$
$$\int 6 = \int 5 + \int 4 - \int 1 = 6 + 7 - 1 = 12,$$
$$\int 7 = \int 6 + \int 5 - \int 2 - \int 0 = 12 + 6 - 3 - 7 = 8,$$
$$\int 8 = \int 7 + \int 6 - \int 3 - \int 1 = 8 + 12 - 4 - 1 = 15,$$
$$\int 9 = \int 8 + \int 7 - \int 4 - \int 2 = 15 + 8 - 7 - 3 = 13,$$
$$\int 10 = \int 9 + \int 8 - \int 5 - \int 3 = 13 + 15 - 6 - 4 = 18,$$
$$\int 11 = \int 10 + \int 9 - \int 6 - \int 4 = 18 + 13 - 12 - 7 = 12,$$
$$\int 12 = \int 11 + \int 10 - \int 7 - \int 5 + \int 0 = 12 + 18 - 8 - 6 + 12 = 28,$$
$$\int 13 = \int 12 + \int 11 - \int 8 - \int 6 + \int 1 = 28 + 12 - 15 - 12 + 1 = 14,$$
$$\int 14 = \int 13 + \int 12 - \int 9 - \int 7 + \int 2 = 14 + 28 - 13 - 8 + 3 = 24,$$
$$\int 15 = \int 14 + \int 13 - \int 10 - \int 8 + \int 3 + \int 0 = 24 + 14 - 18 - 15 + 4 + 15 = 24,$$
$$\int 16 = \int 15 + \int 14 - \int 11 - \int 9 + \int 4 + \int 1 = 24 + 24 - 12 - 13 + 7 + 1 = 31,$$
$$\int 17 = \int 16 + \int 15 - \int 12 - \int 10 + \int 5 + \int 2 = 31 + 24 - 28 - 18 + 6 + 3 = 18,$$
$$\int 18 = \int 17 + \int 16 - \int 13 - \int 11 + \int 6 + \int 3 = 18 + 31 - 14 - 12 + 12 + 4 = 39,$$
$$\int 19 = \int 18 + \int 17 - \int 14 - \int 12 + \int 7 + \int 4 = 39 + 18 - 24 - 28 + 8 + 7 = 20,$$
$$\int 20 = \int 19 + \int 18 - \int 15 - \int 13 + \int 8 + \int 5 = 20 + 39 - 24 - 14 + 15 + 6 = 42.$$

Je crois ces exemples suffisans pour ne pas s'imaginer que c'est par un pur hazard que ma régle se trouve d'accord avec la vérité.

7. Si l'on doutoit encore, si la loi des nombres à retrancher 1, 2, 5, 7, 12, 15, etc. étoit précisement celle que j'ai indiquée, vu que dans les exemples donnés, il n'entre que les six premiers de ces nombres par lesquels la loi ne pourroit pas encore paroitre assez établie, je vai donner quelques exemples de plus grands nombres.

I. Soit proposé le nombre 101 dont on veuille chercher la somme de ses diviseurs, et on aura

$$\begin{aligned}\int 101 &= \int 100 + \int 99 - \int 96 - \int 94 + \int 89 + \int 86 - \int 79 - \int 75 \\ &\quad + \int 66 + \int 61 - \int 50 - \int 44 + \int 31 + \int 24 - \int 9 - \int 1 \\ &= +217 + 156 - 252 - 144 + 90 + 132 - 80 - 124 \\ &\quad + 144 + 62 - 93 - 84 + 32 + 60 - 13 - 1,\end{aligned}$$

ou joignant deux à deux

$$\int 101 = +373 - 396 + 222 - 204 + 206 - 177 + 92 - 14,$$

ce qui donne $\int 101 = 102$, d'où l'on connoitroit que 101 est un nombre premier, si on ne le savoit d'ailleurs.

II. Soit proposé le nombre 301 dont on veut savoir la somme de ses diviseurs, et on aura

$$\begin{aligned}\int 301 &\overset{\text{differ.}}{=} \int 300 \overset{1}{+} \int 299 \overset{3}{-} \int 296 \overset{2}{-} \int 294 \overset{5}{+} \int 289 \overset{3}{+} \int 286 \overset{7}{-} \int 279 \overset{4}{-} \int 275 \\ &\quad \overset{9}{+} \int 266 \overset{5}{+} \int 261 \overset{11}{-} \int 250 \overset{6}{-} \int 244 \overset{13}{+} \int 231 \overset{7}{+} \int 224 \overset{15}{-} \int 209 \overset{8}{-} \int 201 \\ &\quad \overset{17}{+} \int 184 \overset{9}{+} \int 175 \overset{19}{-} \int 156 \overset{10}{-} \int 146 \overset{21}{+} \int 125 \overset{11}{+} \int 114 \overset{23}{-} \int 91 \overset{12}{-} \int 79 \\ &\quad \overset{25}{+} \int 54 \overset{13}{+} \int 41 \overset{27}{-} \int 14 \overset{14}{-} \int 0,\end{aligned}$$

où il est clair, comment par le moyen des differences, on peut aisément former

cette suite pour chaque cas proposé. Or, prenant ces sommes de diviseurs on trouvera

$$\int 301 = +868 - 570 + 307 - 416 + 480 - 468 + 384$$
$$+336 - 684 + 504 - 372 + 390 - 434 + 504$$
$$-240 + 360 - 392 + 156 - 112 + 120 - \ 24$$
$$-272 + 248 - 222 + 240 - \ 80 + \ 42 - 301$$

ou

$$\int 301 = +4939 - 4587 = 352,$$

d'où l'on connoit que 301 n'est pas premier. Or, puisque $301 = 7 \cdot 43$, on aura

$$\int 301 = \int 7 \cdot \int 43 = 8 \cdot 44 = 352,$$

comme la régle vient de montrer.

8. Ces exemples que je viens de déveloper, oteront sans doute tout scrupule qu'on auroit pu encore avoir sur la vérité de ma formule. Or, par là même, on sera d'autant plus surpris de cette belle propriété, ne voyant aucune liaison entre la composition de ma formule et la nature des diviseurs sur la somme desquels roule la proposition. La progression des nombres 1, 2, 5, 7, 12, 15, etc. ne paroit non seulement avoir nul raport au sujet dont il s'agit, mais, comme la loi de ces nombres est interrompuë et qu'ils sont mêlés de deux progressions régulieres differentes, à savoir

de 1, 5, 12, 22, 35, 51, etc. et de 2, 7, 15, 26, 40, 57, etc.,

il semble presque qu'une telle irrégularité ne sauroit trouver lieu dans l'analyse. De plus, le défaut d'une démonstration n'en doit pas peu augmenter la surprise; vu qu'il seroit presque moralement impossible de parvenir à la découverte d'une telle propriété, sans y avoir été conduit par une méthode certaine qui pourroit tenir lieu d'une parfaite démonstration. J'avouë aussi que ce n'a pas été par un pur hazard que je suis tombé sur cette découverte; mais une autre proposition d'une pareille nature qui doit être jugée vraie, quoique je n'en puisse donner une démonstration, m'a ouvert le chemin de parvenir à cette belle propriété. Et bien que cette chose ne roule que sur la nature des nombres à laquelle l'analyse des infinis ne paroit pas être

applicable, c'est pourtant par le moyen des differentiations et plusieurs autres détours que j'ai été conduit à cette conclusion. Je souhaiterois qu'on trouvât un chemin plus court et plus naturel d'y parvenir, et peut-être que la considération de la route que j'ai suivie y pourra conduire.

9. Il y a long-tems[1]) que je considérai, à l'occasion du problème de la partition des nombres, cette expression

$$(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7)(1-x^8) \text{ etc.}$$

La supposant continuée à l'infini, j'ai multiplié actuellement un grand nombre de facteurs ensemble, pour voir la forme de la serie qui en résulteroit, et j'ai trouvé cette progression

$$1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-x^{40}+\text{etc.},$$

où les exposans de x sont les mêmes nombres qui entrent dans la formule précédente; et aussi les signes + et — se trouvent doublés. On n'a qu'à entreprendre cette multiplication et à la continuer aussi loin qu'on jugera à propos, pour se convaincre de la vérité de cette serie. Aussi n'ai-je point d'autre preuve pour cela qu'une longue induction que j'ai du moins poussée si loin, que je ne puis en aucune maniere douter de la loi dont ces termes et leurs exposans sont formés. J'ai long-tems cherché en vain une démonstration rigoureuse que cette serie doit être égale à l'expression proposée $(1-x)(1-x^2)(1-x^3)$ etc. et j'ai proposé la même demande à quelques-uns de mes amis[2]) dont je connois la force dans ces sortes de questions; mais tous sont tombés avec moi d'accord sur la vérité de cette conversion, sans en avoir pu déterrer aucune source de démonstration. Ce sera donc une vérité connuë, mais pas encore démontrée, que si l'on pose

$$s=(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6) \text{ etc.},$$

la même quantité s se pourra aussi exprimer de la sorte

$$s=1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-x^{40}+\text{etc.}$$

1) Voir le mémoire 158 de ce volume, spécialement la note p. 191. F. R.

2) Voir les lettres d'EULER à GOLDBACH du 15 oct. 1743, *Correspondance math. et phys. publiée par. P. H. Fuss*, St.-Pétersbourg 1843, t. I, p. 265, et à NIC. BERNOULLI du 1er sept. et du 10 nov. 1742, *L. Euleri Opera postuma*, t. I, p. 527 et p. 533; les réponses de ces savants se trouvent dans la *Correspondance* citée, t. I, p. 270 et t. II, p. 698; *Leonhardi Euleri Opera omnia*, series III. F. R.

Car chacun est en état de se convaincre de cette vérité par la résolution actuelle à tel point qu'il souhaitera; et il paroit impossible que la loi qu'on a découverte dans 20 termes par exemple, ne soit point observée dans tous les suivans.

10. Ayant donc découvert que ces deux expressions infinies sont égales, quoique l'égalité ne puisse être démontrée, toutes les conclusions qu'on pourra déduire de cette égalité seront de même nature, c'est-à-dire vraies sans être démontrées. Ou, si quelqu'une de ces conclusions pouvoit être démontrée, on en pourroit réciproquement tirer une démonstration de l'égalité mentionnée; et c'est en cette vuë que j'ai manié en plusieurs manieres ces deux expressions, par où j'ai été conduit entre autres à la découverte que je viens d'expliquer, et dont la vérité doit être aussi certaine que celle de l'égalité de ces deux expressions. Voilà de quelle maniere j'ai opéré. Ces deux expressions étant égales

$$\text{I.}\quad s=(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7)\text{ etc.}$$

$$\text{II.}\quad s=1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-x^{40}+\text{etc.},$$

pour délivrer la premiere des facteurs, j'en prends les logarithmes, d'où je tire

$$ls=l(1-x)+l(1-x^2)+l(1-x^3)+l(1-x^4)+l(1-x^5)+\text{etc.}$$

Maintenant, pour éliminer les logarithmes, j'en prends les differentielles, ce qui donnera cette équation

$$\frac{ds}{s}=-\frac{dx}{1-x}-\frac{2xdx}{1-x^2}-\frac{3x^2dx}{1-x^3}-\frac{4x^3dx}{1-x^4}-\frac{5x^4dx}{1-x^5}-\text{etc.}$$

que je divise par $-dx$ et multiplie par x, pour avoir

$$-\frac{xds}{sdx}=\frac{x}{1-x}+\frac{2x^2}{1-x^2}+\frac{3x^3}{1-x^3}+\frac{4x^4}{1-x^4}+\frac{5x^5}{1-x^5}+\text{etc.}$$

La seconde valeur de la même quantité s donne par la differentiation

$$ds=-dx-2xdx+5x^4dx+7x^6dx-12x^{11}dx-15x^{14}dx+\text{etc.},$$

de laquelle, en la multipliant par $-x$ et divisant par sdx, on tirera une autre valeur de $-\frac{xds}{sdx}$ qui sera

$$-\frac{xds}{sdx}=\frac{x+2x^2-5x^5-7x^7+12x^{12}+15x^{15}-22x^{22}-26x^{26}+\text{etc.}}{1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-\text{etc.}}$$

11. Soit la valeur de $-\frac{x\,ds}{s\,dx} = t$, et nous aurons deux valeurs égales pour cette quantité t

$$\text{I.}\quad t = \frac{x}{1-x} + \frac{2x^2}{1-x^2} + \frac{3x^3}{1-x^3} + \frac{4x^4}{1-x^4} + \frac{5x^5}{1-x^5} + \frac{6x^6}{1-x^6} + \text{etc.}$$

$$\text{II.}\quad t = \frac{x + 2x^2 - 5x^5 - 7x^7 + 12x^{12} + 15x^{15} - 22x^{22} - 26x^{26} + \text{etc.}}{1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.}}.$$

De la premiere, je résous chaque terme dans une progression geometrique par la division ordinaire, et j'aurai

$$\begin{array}{lllllllllllll}
t = & x+ & x^2+ & x^3+ & x^4+ & x^5+ & x^6+ & x^7+ & x^8+ & x^9+ & x^{10}+ & x^{11}+ & x^{12}+\text{etc.} \\
 & & +2x^2 & & +2x^4 & & +2x^6 & & +2x^8 & & +2x^{10} & & +2x^{12}+\text{etc.} \\
 & & & +3x^3 & & & +3x^6 & & & +3x^9 & & & +3x^{12}+\text{etc.} \\
 & & & & +4x^4 & & & & +4x^8 & & & & +4x^{12}+\text{etc.} \\
 & & & & & +5x^5 & & & & & +5x^{10} & & +\text{etc.} \\
 & & & & & & +6x^6 & & & & & & +6x^{12}+\text{etc.} \\
 & & & & & & & +7x_7 & & & & & \\
 & & & & & & & & +8x^8 & & & & \\
 & & & & & & & & & +9x^9 & & & \\
 & & & & & & & & & & +10x^{10} & & \\
 & & & & & & & & & & & +11x^{11} & \\
 & & & & & & & & & & & & +12x^{12}+\text{etc.}
\end{array}$$

où il est aisé de voir que chaque puissance de x se trouve autant de fois que son exposant a de diviseurs, puisque chaque diviseur devient un coefficient de la même puissance de x. Ainsi, recueillant tous les termes homogènes dans une somme, le coefficient de chaque puissance de x sera la somme de tous les diviseurs de son exposant. Et partant, exprimant ces sommes de diviseurs par la préposition du signe $\int$, comme j'ai fait ci-dessus, j'obtiendrai pour t la serie qui suit:

$$t = \int 1 \cdot x + \int 2 \cdot x^2 + \int 3 \cdot x^3 + \int 4 \cdot x^4 + \int 5 \cdot x^5 + \int 6 \cdot x^6 + \int 7 \cdot x^7 + \text{etc.}$$

dont la loi de progression est tout à fait manifeste; et, quoiqu'il semble que l'induction ait quelque part dans la détermination de ces coefficiens, qu'on considere l'expression infinie précédente, on s'assurera aisément de la nécessité de cette loi de progression.

12. Substituons cette valeur au lieu de t dans la seconde expression de cette même lettre t qui, étant délivrée de fractions, se réduit en cette forme

$$t(1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.})$$
$$- x - 2x^2 + 5x^5 + 7x^7 - 12x^{12} - 15x^{15} + 22x^{22} + 26x^{26} - \text{etc.} = 0.$$

Maintenant, la valeur précédente de t étant mise dans cette équation, nous trouverons:

$$\begin{aligned} 0 = \int 1 \cdot x + \int 2 \cdot x^2 + \int 3 \cdot x^3 + \int 4 \cdot x^4 + \int 5 \cdot x^5 + \int 6 \cdot x^6 + \int 7 \cdot x^7 + \int 8 \cdot x^8 + \int 9 \cdot x^9 + \text{etc.} \\ - x - \int 1 \cdot x^2 - \int 2 \cdot x^3 - \int 3 \cdot x^4 - \int 4 \cdot x^5 - \int 5 \cdot x^6 - \int 6 \cdot x^7 - \int 7 \cdot x^8 - \int 8 \cdot x^9 - \text{etc.} \\ - 2x^2 - \int 1 \cdot x^3 - \int 2 \cdot x^4 - \int 3 \cdot x^5 - \int 4 \cdot x^6 - \int 5 \cdot x^7 - \int 6 \cdot x^8 - \int 7 \cdot x^9 - \text{etc.} \\ + 5x^5 + \int 1 \cdot x^6 + \int 2 \cdot x^7 + \int 3 \cdot x^8 + \int 4 \cdot x^9 + \text{etc.} \\ + 7x^7 + \int 1 \cdot x^8 + \int 2 \cdot x^9 + \text{etc.} \end{aligned}$$

Ici, il est aisé d'observer que les coefficiens de chaque puissance de x sont les sommes des diviseurs, premierement de l'exposant de cette puissance même, et ensuite des autres nombres plus petits qui résultent si l'on ote successivement de l'exposant les nombres 1, 2, 5, 7, 12, 15, 22, 26, etc. Ensuite, si l'exposant de la puissance de x est égal à un terme de cette serie numerique, alors ce même terme accompagne encore les coefficiens. En troisieme lieu, l'ordre des signes n'a besoin d'aucun éclaircissement. Ainsi, on conclura en général que la puissance x^n aura ces coefficiens:

$$\int n - \int (n-1) - \int (n-2) + \int (n-5) + \int (n-7) - \int (n-12) - \int (n-15) + \text{etc.},$$

jusqu'à ce qu'on parvienne à des nombres négatifs. Mais, si quelqu'un de ces nombres devant lesquels se trouve le signe $\int$ devient $= 0$, alors il faut mettre en sa place le nombre n même, de sorte que dans ce cas, il y a $\int 0 = n$ et le signe de ce terme suit l'ordre général des autres.

13. Puisque donc l'expression infinie du § précédent doit être égale à zero, quelque valeur qu'on donne à la quantité x, il faut de nécessité que les coefficiens de chaque puissance à part, soient égaux ensemble à zero, et partant, nous aurons les équations suivantes:

I.	$\int 1 - 1 = 0,$	ou	$\int 1 = 1,$
II.	$\int 2 - \int 1 - 2 = 0,$		$\int 2 = \int 1 + 2,$
III.	$\int 3 - \int 2 - \int 1 = 0,$		$\int 3 = \int 2 + \int 1,$
IV.	$\int 4 - \int 3 - \int 2 = 0,$		$\int 4 = \int 3 + \int 2,$
V.	$\int 5 - \int 4 - \int 3 + 5 = 0,$		$\int 5 = \int 4 + \int 3 - 5,$
VI.	$\int 6 - \int 5 - \int 4 + \int 1 = 0,$		$\int 6 = \int 5 + \int 4 - \int 1,$
VII.	$\int 7 - \int 6 - \int 5 + \int 2 + 7 = 0,$		$\int 7 = \int 6 + \int 5 - \int 2 - 7,$
	etc.		etc.

et généralement nous aurons:

$$\int n - \int (n-1) - \int (n-2) + \int (n-5) + \int (n-7) - \int (n-12) - \int (n-15) + \text{etc.} = 0$$

et par conséquent

$$\int n = \int (n-1) + \int (n-2) - \int (n-5) - \int (n-7) + \int (n-12) + \int (n-15) - \text{etc.}$$

qui est la même expression que j'ai donnée ci-dessus et qui exprime la loi selon laquelle les sommes des diviseurs des nombres naturels sont continuées. Outre la raison des signes et la nature de la progression des nombres

$$1,\ 2,\ 5,\ 7,\ 12,\ 15,\ 22,\ 26,\ 35,\ 40,\ 51,\ 57,\ 70,\ 77,\ \text{etc.},$$

on voit aussi, par ce que je viens d'avancer, la raison pourquoi, dans les cas où se trouve le terme $\int 0$, il faut mettre en sa place le nombre n même, ce qui auroit pu paroitre le plus étrange dans mon expression. Ce raisonnement, quoiqu'il soit encore fort éloigné d'une démonstration parfaite[1]), ne laissera pas pourtant de lever plusieurs doutes sur la forme bizarre de l'expression que je viens d'expliquer.

1) Voir le mémoire 244 de ce volume. F. R.

DE PARTITIONE NUMERORUM [1]

Commentatio 191 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 3 (1750/1), 1753, p. 125—169
Summarium ibidem p. 15—18

SUMMARIUM

Problema de partitione numerorum Auctori quondam a Cl. Professore Berolinensi NAUDEO fuit oblatum, qui pro casu speciali quaesiverat, quot variis modis numerus 50 in septem partes dispertiri possit. Problema hoc primo intuitu ita comparatum videbatur, ut aliter nisi per inductionem resolvi non posset, quo fere modo pleraque problemata ad artem combinatoriam pertinentia resolvi solent. Qui scilicet eius solutionem suscipere velit, primo quaeret, quot variis modis quisque [numerus] in duas partes discerpi possit, ubi quidem nullam difficultatem offendet; deinde procedet ad divisionem in tres partes, quod negotium etiamnunc satis commode succedet. In divisione in quatuor partes fortasse iam haerebit neque statim perspiciet, quomodo numerus partitionum cum numero partiendo increscat; inductione tamen fretus et hanc progressionis legem divinabit. Quinque-partitio ipsi iam maiores creabit molestias, ac nisi omni circumspectione utatur, verendum est, ne inductioni, utcunque certa ipsi videatur, nimis confidens in errorem inducatur; quod eo magis est pertimescendum in partitione in plures partes, uti etiam ipse problematis Auctor fuit seductus et pro casu proposito in divisione numeri 50 in septem partes post taediosissimos calculos enormiter a veritate aberravit; neque etiam alii insignes Mathematici hac via incedentes ab errore se vindicare valuerunt. Qui autem actu omnes partitiones dinumerare voluerit, non solum in immensum laborem se immergit, sed omni etiam attentione adhibita vix cavebit, ne turpiter decipiatur. Cum igitur hoc problema tam insigne specimen contineat, quam parum in-

1) Vide etiam Commentationes 158 et 394 in hoc vol. 2 et in vol. 3 contentas nec non L. EULERI *Introductionem in analysin infinitorum*, Lausannae 1748, t. I cap. XVI; *LEONHARDI EULERI Opera omnia*, series I, vol. 8. F. R.

ductioni vel maxime confirmatae sit fidendum, eo pluris est aestimandum Auctoris studium, quo certa methodo solutionem istius problematis investigavit, cum vix ulla alia via praeter inductionem ad eam patere videatur.

Nihil igitur inductioni tribuens Auctor ex certissimis Analyseos principiis eiusmodi formulas hausit, quae pro quocunque numero proposito statim ostendunt, quot variis modis is in tot, quot lubuerit, partes dividi possit, ita, ut etiam circa maximos numeros nullum dubium superesse queat. Problema autem hic geminum tractat, quorum altero quaeritur, quot modis datus numerus in tot partes inaequales tantum, quot requiruntur, dissecari possit, in altero vero partium aequalitas non excluditur. Ita in exemplo initio memorato invenit numerum 50 omnino 522 modis in septem partes inter se inaequales distribui posse, aequalitate autem partium non exclusa numerum partitionum omnium esse 8946, qui ergo numerus quaestioni primum propositae satisfacit.

Pluribus aliis modis problema variari potest, dum scilicet singulae partes datae indolis esse iubentur, veluti numeri impares vel quadrati vel termini progressionis geometricae duplae etc. partium numero vel praescripto vel secus; Auctoris autem methodus aeque patet ad omnia huiusmodi problemata solvenda.

Subiungit denique Auctor tabulam satis amplam, ex qua responsiones ad plerasque huius generis quaestiones sine ullo labore depromere licet; quae multo longius est continuata, quam in Auctoris *Introductione in Analysin*, ubi idem argumentum iam tractaverat, hic autem studiosius expolivit. Ceterum haec Dissertatio referta est plurimis tam egregiis artificiis quam novis et notatu dignis observationibus circa naturam serierum, unde eius usus multo latius patere videtur; neque ullum est dubium, quin ex eodem fonte plurima alia argumenta felicissimo cum successu expediri queant. [1])

1. Problema *de partitione numerorum* primum mihi est propositum a Celeb. Professore NAUDE[2]), in quo quaerebat, quot variis modis datus numerus integer (hic enim perpetuo de numeris tantum integris et affirmativis est sermo) possit esse aggregatum duorum vel trium vel quatuor vel in genere quot libuerit numerorum. Sive, quod eodem redit, quaeritur, quot variis modis datus numerus vel in duas vel tres vel quatuor vel quot libuerit partes dispertiri queat, unde huic problemati aptissime *partitionis numerorum*

1) In editione principe hic sequitur index errorum, qui inveniuntur in commentatione. Qui errores hac in editione correcti sunt. F. R.

2) Vide notam p. 178. F. R.

nomen est impositum. Bipartitum autem hoc problema a Viro Celeb. proponi solet: primo scilicet eos tantum partitionis modos postulat, quibus singulae partes, in quas numerus propositus resolvitur, sint inter se inaequales; tum vero hac inaequalitatis conditione omissa omnes omnino partitionis modos requirit, sive partes quaepiam inter se fuerint aequales sive omnes inaequales. Perspicuum autem est hoc posteriori casu numerum partitionum plerumque multo esse maiorem quam priori, cum non solum omnes partitiones, quae casui priori satisfaciunt, simul posteriorem resolvant, sed etiam plerumque plures alii accedant, in quibus partes aequales contineantur.

2. Ut vis problematis huius clarius perspiciatur, nonnullos casus simpliciores [afferam], qui actuali partitionum enumeratione facile expediuntur. Si quaeratur, quot variis modis numerus 6 in duas partes resolvi possit, statim apparet hoc tribus modis fieri posse, cum sit

$$6 = 1 + 5 = 2 + 4 = 3 + 3,$$

siquidem partium aequalitas non excludatur. Sin autem partes tantum inaequales desiderentur, ultima partitio $3 + 3$ est omittenda hocque casu numerus 6 duobus tantum modis in duas partes inter se inaequales dispertiri potest. Quodsi numerus impar, uti 9, proponatur in duas partes distribuendus, quatuor prodibunt partitiones, quae sunt

$$9 = 1 + 8 = 2 + 7 = 3 + 6 = 4 + 5;$$

ubi cum partes aequales non occurrant, numerus 9 quatuor modis in duas partes dispertietur, sive partes aequales excludantur sive secus. Si plures duabus partes desiderentur, uti si quaeratur, quot variis modis numerus 12 in tres partes dispertiri possit, hoc sequentibus 12 modis fieri poterit:

$$\begin{array}{lll} 12 = 1 + 1 + 10, & 12 = 1 + 2 + 9, & 12 = 1 + 3 + 8, \\ 12 = 1 + 4 + \ \ 7, & 12 = 1 + 5 + 6, & 12 = 2 + 2 + 8, \\ 12 = 2 + 3 + \ \ 7, & 12 = 2 + 4 + 6, & 12 = 2 + 5 + 5, \\ 12 = 3 + 3 + \ \ 6, & 12 = 3 + 4 + 5, & 12 = 4 + 4 + 4. \end{array}$$

Sin autem partes aequales excludantur, respondendum erit numerum 12 tantum 7 modis in tres partes distribui posse.

3. Hinc facile intelligitur, si tam numerus dispertiendus fuerit maior atque numerus partium, in quas eum resolvi oportet, ternarium quaternariumve superet, numerum partitionum tam fieri magnum, ut per enumerationem actu instituendam difficillime obtineri queat. Neque etiam in hoc negotio inductioni multum est fidendum, quae, uti periculum facienti facile patebit, plerumque fallit, si ab enumeratione pro casibus simplicioribus facta ad magis compositos conclusiones formare voluerit. Sic ex methodo post explicanda patebit numerum 50 in septem partes non exclusa partium aequalitate dispertiri posse 8946 modis; sin autem partes aequales excludantur, remanebunt tantum 522 partitiones. Numerus porro 42 mille diversis modis in 20 partes omnino resolvi potest. At si quaeratur, quot variis modis numerus 125 in 12 partes, quae sint inter se omnes inaequales, distribui possit, reperietur hoc fieri posse 64707 modis.

4. Quemadmodum hic omnes numeri integri partium loca tenere possint, ita hoc problema in infinitum variari potest, prout numeri partes constituentes restringuntur. Ita aliud erit problema, si quaeratur, quot variis modis datus numerus n in p partes, quarum nulla datum numerum m excedat, resolvi possit. Partium quoque numerus omitti potest[1]), uti si quaeratur, quot variis modis numerus 6 ex his numeris 1, 2, 3, 4 per additionem produci possit, quod sequentibus 9 modis fieri poterit:

$$6 = 1 + 1 + 1 + 1 + 1 + 1, \qquad 6 = 1 + 1 + 1 + 3,$$
$$6 = 1 + 1 + 1 + 1 + 2, \qquad 6 = 1 + 1 + 4,$$
$$6 = 1 + 1 + 2 + 2, \qquad 6 = 1 + 2 + 3,$$
$$6 = 2 + 2 + 2, \qquad 6 = 2 + 4,$$
$$6 = 3 + 3.$$

Vel etiam qualitas numerorum praescribi potest, qui partes constituant; uti si partes debeant esse vel numeri impares vel quadrati vel triangulares vel alius cuiusque generis. Sic si quaeratur, quot variis modis datus numerus possit esse summa quatuor quadratorum, quaestio ad hoc genus pertinebit. Iam pridem quoque partitio numerorum omnium in partes, quae sint termini

1) Vide D. MAHNKE, *Leibniz auf der Suche nach einer allgemeinen Primzahlgleichung*, Biblioth. Mathem. 13_3, 1912/3, p. 29, imprimis p. 37. F. R.

huius progressionis geometricae 1, 2, 4, 8, 16, 32 etc., est considerata et quilibet numerus observatus est unico tantum modo ex his numeris 1, 2, 4, 8, 16, 32 etc. per additionem componi posse. Cuius quaestionis post STIFELIUM[1]) mentionem facit SCHOTENIUS[2]) in suis *Exercitationibus*, ubi ostendit pondera 1, 2, 4, 8, 16, 32 etc. librarum sufficere posse ad merces quotcunque librarum inponderandas.[3]) Neque vero ad hoc ostendendum alia methodo praeter inductionem utitur. Quamobrem non abs re erit veritatem huius effati rigorose demonstrasse.

5. Quemadmodum ergo haec aliaque similia problemata resolvi oporteat, hic eiusmodi methodum certam ac tutam proponam, ut inductione, cui vulgo ad solutionem istiusmodi quaestionum plurimum tribui solet, plane non sit opus. Utor ad hoc sequenti lemmate notissimo:

Si istud productum

$$(1+az)(1+bz)(1+cz)(1+dz)(1+ez) \text{ etc.},$$

sive factorum numerus sit finitus sive infinitus, per actualem multiplicationem evolvatur, ut huiusmodi forma prodeat

$$1+Az+Bz^2+Cz^3+Dz^4+Ez^5+\text{etc.},$$

erit coefficiens secundi termini A summa quantitatum omnium a, b, c, d, e etc. Coefficiens vero B erit summa productorum ex binis harum quantitatum inaequalibus. Coefficiens C erit summa productorum ex ternis istarum quantitatum inaequalibus; et coefficiens D erit summa productorum ex quaternis harum earundem quantitatum, et ita porro.

In huiusmodi enim productis eadem quantitas, puta a, vel quaevis alia plus quam semel nusquam inesse potest. Unde hoc lemma mihi fundamentum suppeditat ad partitiones in partes inaequales.

1) M. STIFEL, *Die Coss Christoffs Rudolffs*, Königsperg 1553, fol 11'. F. R.

2) Fr. v. SCHOOTEN, *Exercitationum mathematicarum libri quinque*, Lugd. Batav. 1657, lib. V sectio VIII, p. 410. F. R.

3) Id quod iam docuit LEONARDO PISANO; vide G. ENESTRÖM, *Über die ältere Geschichte der Zerfällung ganzer Zahlen in Summen kleinerer Zahlen*, Biblioth. Mathem. 13_3, 1912/3, p. 352. F. R.

6. Sin autem aequalitas partium non excludatur, adhibeo hoc lemma:

Si ista formula

$$\frac{1}{(1-az)(1-bz)(1-cz)(1-dz)(1-ez)\text{ etc.}},$$

sive factorum denominatorem constituentium numerus sit finitus sive infinitus, post evolutionem denominatoris ope multiplicationis factam per divisionem in seriem explicetur huius formae

$$1+Az+Bz^2+Cz^3+Dz^4+Ez^5+\text{etc.},$$

tum erit A quidem ut ante summa quantitatum $a+b+c+d+e+\text{etc.}$ *At coefficiens B erit summa productorum ex binis harum quantitatum non exclusa repetitione eiusdem quantitatis, erit scilicet*

$$B=aa+ab+bb+ac+bc+cc+ad+bd+cd+dd+ae+\text{etc.}$$

Simili modo coefficiens C erit summa productorum ex ternis harum quantitatum a, b, c, d, e etc. factoribus aequalibus in quovis producto non exclusis. Atque eadem conditione adiecta erit coefficiens D summa productorum ex quaternis harum quantitatum, et ita porro.

Hincque istud lemma viam aperiet ad partitiones, in quibus partium aequalitas non excluditur, absolvendas.

7. Cum autem in problemate proposito non de productis, sed de summis numerorum quaestio instituatur, loco quantitatum a, b, c, d, e etc. substituo potestates x^p, x^q, x^r, x^s, x^t etc. Sic enim in productis ex binis eiusmodi occurrent potestates, quarum exponentes sint summae binarum ex serie p, q, r, s, t etc. Simili modo producta ex ternis constant eiusmodi potestatibus, quarum exponentes sint summae trium numerorum ex eadem serie p, q, r, s etc. Atque producta ex quaternis erunt potestates, quarum exponentes sint aggregata ex quaternis horum numerorum, et ita porro. Sicque, quae ante de productis sunt notata, nunc ad summas transferuntur et ita quidem, ut, si lemma prius adhibeatur, summae ex partibus tantum inaequalibus conflentur, sin autem lemma posterius in usum vocetur, partium aequalitas non excludatur. Hoc igitur modo ambo lemmata ad solutionem quaestionum ante memoratarum accommodari debebunt.

8. Aggrediamur ergo hanc primam quaestionem:

Invenire, quot variis modis datus numerus N possit dispertiri in p partes, quae sint inter se inaequales.

Quoniam huc omnes numeri integri affirmativi ad partes constituendas sunt idonei, pro serie superiorum exponentium accipienda est series numerorum naturalium 1, 2, 3, 4, 5, 6 etc. Formetur ergo secundum lemma prius haec expressio

$$s = (1 + xz)(1 + x^2z)(1 + x^3z)(1 + x^4z)(1 + x^5z) \text{ etc. in infinitum,}$$

quae multiplicatione actu instituta evolvatur in hanc seriem

$$s = 1 + Az + Bz^2 + Cz^3 + Dz^4 + Ez^5 + \text{etc.},$$

eritque

$$A = x^1 + x^2 + x^3 + x^4 + x^5 + x^6 + \text{etc.},$$

quod est aggregatum omnium potestatum ipsius x. Deinde quia B est summa productorum ex binis terminis inaequalibus seriei A, erit B summa potestatum ipsius x omnium, quarum exponentes sint aggregata duorum numerorum inaequalium; et cum eadem potestas saepius resultare possit, ea unciam habebit numericam indicantem, quot ea potestas modis sit productum ex duobus terminis seriei A seu quot variis modis eius exponens possit esse summa duorum numerorum inaequalium. Binis autem terminis seriei A re ipsa multiplicandis reperietur

$$B = x^3 + x^4 + 2x^5 + 2x^6 + 3x^7 + 3x^8 + 4x^9 + 4x^{10} + \text{etc.}$$

Cuius seriei quilibet coefficiens indicat, quot variis modis exponens potestatis ipsius x adiunctae in duas partes inaequales dispertiri possit. Hac igitur serie in infinitum continuata ope legis post eruendae resolvitur problematis propositi casus, quo partitio in duas partes requiritur.

9. Quantitas deinde C, cum contineat omnia producta, quae oriuntur ternis terminis inaequalibus seriei A invicem multiplicandis, constabit ex serie potestatum ipsius x, quarum exponentes sunt summae trium numerorum inter se inaequalium. Atque eadem potestas toties in ista serie C occurret, quoties eius exponens ex tribus numeris inter se inaequalibus per additionem resultare poterit, reperieturque

$$C = x^6 + x^7 + 2x^8 + 3x^9 + 4x^{10} + 5x^{11} + 7x^{12} + 8x^{13} + 10x^{14} + \text{etc.}$$

Cuius seriei quilibet coefficiens indicat, quot variis modis exponens potestatis ipsius x adiunctae in tres partes inaequales dispertiri possit; sic ex termino $8x^{13}$ colligitur numerum 13 octo diversis modis in tres partes inaequales secari posse, quae sunt

$$\begin{array}{ll} 13 = 1 + 2 + 10, & 13 = 2 + 3 + 8, \\ 13 = 1 + 3 + 9, & 13 = 2 + 4 + 7, \\ 13 = 1 + 4 + 8, & 13 = 2 + 5 + 6, \\ 13 = 1 + 5 + 7, & 13 = 3 + 4 + 6. \end{array}$$

Ista igitur series C in infinitum continuata inserviet omnibus numeris in tres partes inaequales dispertiendis.

10. Quantitas porro D, cum contineat omnia producta ex quaternis terminis inaequalibus seriei $A = x^1 + x^2 + x^3 + x^4 + \text{etc.}$, constabit serie potestatum ipsius x, quarum exponentes sint aggregata quatuor numerorum inter se inaequalium; et in hac serie quaelibet potestas eiusmodi habebit coefficientem, qui indicat, quot variis modis eius exponens per additionem quatuor numerorum inter se inaequalium resultare possit. Reperietur autem

$$D = x^{10} + x^{11} + 2x^{12} + 3x^{13} + 5x^{14} + 6x^{15} + 9x^{16} + 11x^{17} + \text{etc.}$$

Haec igitur series in infinitum continuata ostendet, quot variis modis quisque numerus possit esse summa quatuor numerorum inaequalium. Ex termino quippe $9x^{16}$ cognoscitur numerum 16 novem modis in quatuor partes inter se inaequales distribui posse.

11. Si hoc modo ulterius progrediamur, patebit litteram E fore seriem potestatum ipsius x ita comparatam, ut cuiusvis termini coefficiens indicet, quot variis modis exponens ipsius x in quinque partes inaequales dissecari possit. Erit autem

$$E = x^{15} + x^{16} + 2x^{17} + 3x^{18} + 5x^{19} + 7x^{20} + 10x^{21} + 13x^{22} + \text{etc.}$$

Simili modo valor litterae F erit series partitionibus in sex partes inaequales inserviens et litterae G, H, I etc. pro partitionibus in partes septem, octo, novem etc. valebunt eruntque

8. Aggrediamur ergo hanc primam quaestionem:

Invenire, quot variis modis datus numerus N possit dispertiri in p partes, quae sint inter se inaequales.

Quoniam huc omnes numeri integri affirmativi ad partes constituendas sunt idonei, pro serie superiorum exponentium accipienda est series numerorum naturalium 1, 2, 3, 4, 5, 6 etc. Formetur ergo secundum lemma prius haec expressio

$$s = (1 + xz)(1 + x^2 z)(1 + x^3 z)(1 + x^4 z)(1 + x^5 z) \text{ etc. in infinitum,}$$

quae multiplicatione actu instituta evolvatur in hanc seriem

$$s = 1 + Az + Bz^2 + Cz^3 + Dz^4 + Ez^5 + \text{etc.},$$

eritque

$$A = x^1 + x^2 + x^3 + x^4 + x^5 + x^6 + \text{etc.},$$

quod est aggregatum omnium potestatum ipsius x. Deinde quia B est summa productorum ex binis terminis inaequalibus seriei A, erit B summa potestatum ipsius x omnium, quarum exponentes sint aggregata duorum numerorum inaequalium; et cum eadem potestas saepius resultare possit, ea unciam habebit numericam indicantem, quot ea potestas modis sit productum ex duobus terminis seriei A seu quot variis modis eius exponens possit esse summa duorum numerorum inaequalium. Binis autem terminis seriei A re ipsa multiplicandis reperietur

$$B = x^3 + x^4 + 2x^5 + 2x^6 + 3x^7 + 3x^8 + 4x^9 + 4x^{10} + \text{etc.}$$

Cuius seriei quilibet coefficiens indicat, quot variis modis exponens potestatis ipsius x adiunctae in duas partes inaequales dispertiri possit. Hac igitur serie in infinitum continuata ope legis post eruendae resolvitur problematis propositi casus, quo partitio in duas partes requiritur.

9. Quantitas deinde C, cum contineat omnia producta, quae oriuntur ternis terminis inaequalibus seriei A invicem multiplicandis, constabit ex serie potestatum ipsius x, quarum exponentes sunt summae trium numerorum inter se inaequalium. Atque eadem potestas toties in ista serie C occurret, quoties eius exponens ex tribus numeris inter se inaequalibus per additionem resultare poterit, reperieturque

$$C = x^6 + x^7 + 2x^8 + 3x^9 + 4x^{10} + 5x^{11} + 7x^{12} + 8x^{13} + 10x^{14} + \text{etc.}$$

Cuius seriei quilibet coefficiens indicat, quot variis modis exponens potestatis ipsius x adiunctae in tres partes inaequales dispertiri possit; sic ex termino $8x^{13}$ colligitur numerum 13 octo diversis modis in tres partes inaequales secari posse, quae sunt

$$13 = 1 + 2 + 10, \qquad 13 = 2 + 3 + 8,$$
$$13 = 1 + 3 + 9, \qquad 13 = 2 + 4 + 7,$$
$$13 = 1 + 4 + 8, \qquad 13 = 2 + 5 + 6,$$
$$13 = 1 + 5 + 7, \qquad 13 = 3 + 4 + 6.$$

Ista igitur series C in infinitum continuata inserviet omnibus numeris in tres partes inaequales dispertiendis.

10. Quantitas porro D, cum contineat omnia producta ex quaternis terminis inaequalibus seriei $A = x^1 + x^2 + x^3 + x^4 + \text{etc.}$, constabit serie potestatum ipsius x, quarum exponentes sint aggregata quatuor numerorum inter se inaequalium; et in hac serie quaelibet potestas eiusmodi habebit coefficientem, qui indicat, quot variis modis eius exponens per additionem quatuor numerorum inter se inaequalium resultare possit. Reperietur autem

$$D = x^{10} + x^{11} + 2x^{12} + 3x^{13} + 5x^{14} + 6x^{15} + 9x^{16} + 11x^{17} + \text{etc.}$$

Haec igitur series in infinitum continuata ostendet, quot variis modis quisque numerus possit esse summa quatuor numerorum inaequalium. Ex termino quippe $9x^{16}$ cognoscitur numerum 16 novem modis in quatuor partes inter se inaequales distribui posse.

11. Si hoc modo ulterius progrediamur, patebit litteram E fore seriem potestatum ipsius x ita comparatam, ut cuiusvis termini coefficiens indicet, quot variis modis exponens ipsius x in quinque partes inaequales dissecari possit. Erit autem

$$E = x^{15} + x^{16} + 2x^{17} + 3x^{18} + 5x^{19} + 7x^{20} + 10x^{21} + 13x^{22} + \text{etc.}$$

Simili modo valor litterae F erit series partitionibus in sex partes inaequales inserviens et litterae G, H, I etc. pro partitionibus in partes septem, octo, novem etc. valebunt eruntque

$$F = x^{21} + x^{22} + 2x^{23} + 3x^{24} + 5x^{25} + 7x^{26} + 11x^{27} + 14x^{28} + \text{etc.},$$
$$G = x^{28} + x^{29} + 2x^{30} + 3x^{31} + 5x^{32} + 7x^{33} + 11x^{34} + 15x^{35} + \text{etc.}$$

etc.

Unde perspicitur primi cuiusque seriei termini exponentem esse numerum trigonalem numeri partium propositi, tum vero tam huius quam secundi termini coefficientem esse $= 1$. Cuius quidem ratio facile intelligitur; minimus enim numerus, qui est summa septem numerorum inter se inaequalium, necessario est $= 1 + 2 + 3 + 4 + 5 + 6 + 7 = \frac{1}{2}7 \cdot 8 =$ numero trigonali ipsius septenarii hicque numerus pariter ac sequens unitate maior plus uno modo in septem partes inaequales dispertiri nequit.

12. Totum ergo negotium redit ad commodam serierum B, C, D, E, F etc. formationem, ne id ipsum, quod quaeritur, scilicet partitionum numerus, ad cuiusque seriei formationem adhibeatur. Ac primo quidem lex progressionum A et B est aperta, cum prioris coefficientes sint omnes unitates, posterioris vero termini seriei numerorum naturalium geminati; sequentium vero serierum lex minus est aperta, et quousque eas hic continuavimus, coefficientes ex ipsis cuiusque exponentis partitionibus constituimus. Alio itaque modo valores istarum litterarum A, B, C, D etc. investigari oportet, unde haec exoritur quaestio:

Invenire valores litterarum A, B, C, D, E etc., ita ut summa huius seriei

$$s = 1 + Az + Bz^2 + Cz^3 + Dz^4 + Ez^5 + \text{etc.}$$

aequalis fiat isti expressioni

$$s = (1 + xz)(1 + x^2z)(1 + x^3z)(1 + x^4z)(1 + x^5z) \text{ etc.}$$

Hunc in finem igitur perpendendus est nexus, qui inter has duas expressiones intercedit, et quemadmodum altera immutari debeat, si in altera mutatio instituatur.

13. Quia utriusque expressionis idem est valor s, ambae inter se manebunt aequales, si in utraque loco z scribatur quaecunque alia quantitas. Ponamus igitur in utraque xz loco z et valor utrinque resultans vocetur t eritque primo

$$t = 1 + Axz + Bx^2z^2 + Cx^3z^3 + Dx^4z^4 + \text{etc.};$$

tum vero altera expressio transmutabitur in hanc

$$t = (1 + x^2 z)(1 + x^3 z)(1 + x^4 z)(1 + x^5 z) \text{ etc.};$$

qui posterior ipsius t valor si cum posteriore valore ipsius s comparetur, quo erat

$$s = (1 + xz)(1 + x^2 z)(1 + x^3 z)(1 + x^4 z) \text{ etc.},$$

mox patebit esse $s = (1 + xz)t$. Quae relatio cum etiam in alteris valoribus ipsarum s et t locum habere debeat, nobis praebebit hanc aequationem

$$\begin{aligned} s &= 1 + A\,z + B\,z^2 + C\,z^3 + D\,z^4 + \text{etc.}, \\ (1 + xz)t &= 1 + Axz + Bx^2z^2 + Cx^3z^3 + Dx^4z^4 + \text{etc.} \\ &\quad + xz + Ax^2z^2 + Bx^3z^3 + Cx^4z^4 + \text{etc.} \end{aligned}$$

Unde terminis homogeneis inter se aequandis fiet

$$\begin{aligned} A &= \frac{x}{1-x}, \\ B &= \frac{Ax^2}{1-x^2} = \frac{x^3}{(1-x)(1-x^2)}, \\ C &= \frac{Bx^3}{1-x^3} = \frac{x^6}{(1-x)(1-x^2)(1-x^3)}, \\ D &= \frac{Cx^4}{1-x^4} = \frac{x^{10}}{(1-x)(1-x^2)(1-x^3)(1-x^4)}, \\ E &= \frac{Dx^5}{1-x^5} = \frac{x^{15}}{(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)} \\ &\text{etc.} \end{aligned}$$

14. Series ergo, quae supra pro litteris A, B, C, D, E etc. prodire observatae sunt, oriuntur ex evolutione fractionum, quas hic invenimus, unde constat seriem A esse geometricam, nempe $A = x + x^2 + x^3 + x^4 + x^5 + \text{etc.}$, quae, quod quidem est planissimum, indicat quemque numerum unico modo ex uno numero integro constare. Reliquae vero series B, C, D, E etc. sunt recurrentes, quarum scala relationis ex cuiusvis fractionis denominatore per multiplicationem evoluto patebit. Ad hoc ostendendum negligamus tantisper numeratores, qui sunt potestates ipsius x, quarum exponentes sunt

numeri trigonales, earumque loco scribamus unitatem. Sit igitur

$$\frac{A}{x} = 1 + \alpha' x + \beta' x^2 + \gamma' x^3 + \delta' x^4 + \varepsilon' x^5 + \cdots + v' x^n + \cdots = \mathfrak{A},$$

$$\frac{B}{x^3} = 1 + \alpha'' x + \beta'' x^2 + \gamma'' x^3 + \delta'' x^4 + \varepsilon'' x^5 + \cdots + v'' x^n + \cdots = \mathfrak{B},$$

$$\frac{C}{x^6} = 1 + \alpha''' x + \beta''' x^2 + \gamma''' x^3 + \delta''' x^4 + \varepsilon''' x^5 + \cdots + v''' x^n + \cdots = \mathfrak{C},$$

$$\frac{D}{x^{10}} = 1 + \alpha^{IV} x + \beta^{IV} x^2 + \gamma^{IV} x^3 + \delta^{IV} x^4 + \varepsilon^{IV} x^5 + \cdots + v^{IV} x^n + \cdots = \mathfrak{D},$$

$$\frac{E}{x^{15}} = 1 + \alpha^{V} x + \beta^{V} x^2 + \gamma^{V} x^3 + \delta^{V} x^4 + \varepsilon^{V} x^5 + \cdots + v^{V} x^n + \cdots = \mathfrak{E},$$

$$\frac{F}{x^{21}} = 1 + \alpha^{VI} x + \beta^{VI} x^2 + \gamma^{VI} x^3 + \delta^{VI} x^4 + \varepsilon^{VI} x^5 + \cdots + v^{VI} x^n + \cdots = \mathfrak{F}$$

etc.

15. Solutio ergo quaestionis ad inventionem seriërum $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, $\mathfrak{E}$ etc. reducitur, quas patet singulas esse recurrentes. Ac primo quidem series $\mathfrak{A}$, cum sit $\mathfrak{A} = \frac{1}{1-x}$, est adeo geometrica, atque $\alpha' = 1$, $\beta' = 1$, $\gamma' = 1$, $\delta' = 1$ etc., quod per se est perspicuum. Series autem $\mathfrak{B}$, cum sit

$$\mathfrak{B} = \frac{1}{(1-x)(1-x^2)} = \frac{1}{1-x-x^2+x^3},$$

erit recurrens scala relationis existente $+1$, $+1$, -1; unde erit

$$\begin{aligned}
\alpha'' &= 1,\\
\beta'' &= \alpha'' + 1,\\
\gamma'' &= \beta'' + \alpha'' - 1,\\
\delta'' &= \gamma'' + \beta'' - \alpha'',\\
\varepsilon'' &= \delta'' + \gamma'' - \beta'',\\
\zeta'' &= \varepsilon'' + \delta'' - \gamma''
\end{aligned}$$

etc.

Simili modo series $\mathfrak{C}$ ob

$$\mathfrak{C} = \frac{1}{(1-x)(1-x^2)(1-x^3)} = \frac{1}{1-x-x^2+x^4+x^5-x^6}$$

erit recurrens et scalam relationis habebit $+1,\ +1,\ 0,\ -1,\ -1,\ +1$. Unde erit

$$\begin{aligned}
\alpha''' &= 1,\\
\beta''' &= \alpha''' + 1,\\
\gamma''' &= \beta''' + \alpha''' + *,\\
\delta''' &= \gamma''' + \beta''' + * - 1,\\
\varepsilon''' &= \delta''' + \gamma''' + * - \alpha''' - 1,\\
\zeta''' &= \varepsilon''' + \delta''' + * - \beta''' - \alpha''' + 1,\\
\eta''' &= \zeta''' + \varepsilon''' + * - \gamma''' - \beta''' + \alpha''',\\
\theta''' &= \eta''' + \zeta''' + * - \delta''' - \gamma''' + \beta'''
\end{aligned}$$

etc.

Eodem modo series sequentes perspicientur esse recurrentes singularumque scalae relationis hoc modo assignari poterunt. Etsi autem hoc pacto istae series non difficulter formari possunt, tamen ista ratione relicta mox multo commodiorem modum exhibebo harum serierum quamvis ex praecedente formandi, postquam observationem maximi momenti communicavero.

16. Cum sit $\mathfrak{B} = \frac{1}{(1-x)(1-x^2)}$, patet in serie evoluta $\mathfrak{B}$ quamvis potestatem ipsius x toties occurrere debere, quoties ea ex potestatibus x^1, x^2 per multiplicationem oriri potest seu quoties eius exponens ex numeris 1 et 2 per additionem produci potest. Ita cum sit

$$\mathfrak{B} = 1 + x + 2x^2 + 2x^3 + 3x^4 + 3x^5 + \cdots + v''x^n + \cdots,$$

ex termino $3x^4$ intelligitur numerum 4 tribus modis ex numeris 1 et 2 per additionem oriri posse, qui sunt

$$4 = 1 + 1 + 1 + 1, \quad 4 = 1 + 1 + 2 \quad \text{et} \quad 4 = 2 + 2.$$

In genere ergo terminum $v''x^n$ considerando coefficiens v'' indicabit, quot modis exponens n ex numeris 1 et 2 per additionem produci possit. Cum igitur sit $B = \mathfrak{B}x^3$, in serie B habebitur iste terminus $v''x^{n+3}$; qui cum indicet numerum $n+3$ tot variis modis in duas partes inaequales secari

posse, quot unitates coefficiens v'' in se complectatur, manifestum est numerum $n+3$ tot modis in duas partes inaequales distribui posse, quot modis numerus n ex numeris 1 et 2 per additionem produci queat.

17. Deinde cum sit $\mathfrak{C} = \frac{1}{(1-x)(1-x^2)(1-x^3)}$, patet in hac serie $\mathfrak{C}$ quamvis potestatem ipsius x toties occurrere debere, quoties ea ex potestatibus x^1, x^2, x^3 per multiplicationem oriri queat seu, quod idem est, quoties eius exponens ex numeris 1, 2, 3 per additionem produci possit. Ita cum sit

$$\mathfrak{C} = 1 + x + 2x^2 + 3x^3 + 4x^4 + 5x^5 + 7x^6 + \cdots + v'''x^n + \cdots,$$

ex quovis eius termino $5x^5$ cognoscetur exponentem 5 quinque modis ex numeris 1, 2, 3 per additionem produci posse, qui sunt

$$5 = 1+1+1+1+1, \quad 5 = 1+1+1+2, \quad 5 = 1+1+3,$$
$$5 = 1+2+2, \quad 5 = 2+3.$$

In genere autem terminum $v'''x^n$ considerando coefficiens v''' indicabit, quot variis modis numerus n ex numeris 1, 2, 3 per additionem oriri queat. Cum igitur sit $C = \mathfrak{C}x^6$, in serie C habebitur iste terminus $v'''x^{n+6}$, quo indicatur numerum $n+6$ tot modis, quot unitates continentur in coefficiente v''', in tres partes inaequales dispertiri posse. Unde consequitur numerum $n+6$ totidem modis in tres partes inaequales distribui posse, quot modis numerus n ex numeris 1, 2, 3 per additionem produci possit.

18. Non opus est, ut hoc ratiocinium longius prosequamur, cum hinc iam abunde perspiciatur quemvis numerum $n+10$ tot variis modis in quatuor partes inaequales dispertiri posse, quot modis numerus n ex his quatuor numeris 1, 2, 3, 4 per additionem produci possit. Simili modo quilibet numerus $n+15$ tot variis modis in quinque partes inaequales dispertiri poterit, quot modis numerus n ex his quinque numeris 1, 2, 3, 4, 5 per additionem produci potest. Generatim ergo numerus $n + \frac{m(m+1)}{2}$ tot variis modis in m partes inaequales dispertiri poterit, quot variis modis numerus n ex his numeris 1, 2, 3, 4, ... m per additionem produci potest. Quodsi ergo quaeratur, quot variis modis numerus N in m partes inaequales dispertiri possit, responsio reperietur, si casuum numerus investigetur, quibus numerus $N - \frac{m(m+1)}{2}$ ex numeris 1, 2, 3, 4, ... m per additionem produci potest.

19. Hoc igitur modo resolutio quaestionis propositae de partitione cuiusque numeri in quot libuerit partes inaequales reducitur ad solutionem alius problematis iam supra commemorati, quo quaeritur, quot variis modis quilibet numerus ex aliquot terminis huius progressionis arithmeticae 1, 2, 3, 4, 5 etc. per additionem produci possit. Hacque posteriore quaestione resoluta simul prior resolvetur. Quod ut clarius explicemus, nova signa ad commodiorem expressionem adhibeamus. Denotet ergo haec scriptio:

$n^{(2)}$ numerum casuum, quibus numerus n ex duobus numeris 1, 2 per additionem formari possit;

$n^{(3)}$ denotet numerum casuum, quibus numerus n ex his numeris 1, 2, 3 per additionem formari possit;

et $n^{(m)}$ denotet numerum casuum, quibus numerus n ex his numeris 1, 2, 3, ... m per additionem produci possit.

Cum igitur valores huiusmodi characterum fuerint definiti, quod deinceps praestabimus, problema propositum ita resolvetur. Si quaeratur scilicet, quot variis modis numerus N in m partes inaequales dispertiri possit, numerus casuum quaesitus exprimetur hoc charactere $\left(N-\frac{m(m+1)}{1\cdot 2}\right)^{(m)}$, quippe quo indicatur, quot variis modis numerus $N-\frac{m(m+1)}{2}$ ex his numeris 1, 2, 3, ... m per additionem produci possit.

20. Ad hanc eandem quaestionem quoque reducitur solutio alterius problematis a Celeb. Naudeo propositi, quamobrem expediet et hoc problema ante resolvi, quam ampliorem characterum modo assumtorum evolutionem suscipiamus; sic enim tria problemata, quae inter se maxime videantur diversa, una eademque opera resolvemus. Problema autem ita se habet:

Invenire, quot variis modis datus numerus N possit dispertiri in p partes partium aequalitate non exclusa.

Quoniam hic partium aequalitas non excluditur, sequentem formam contemplabor, quae huius quaestionis solutionem in se continebit,

$$s=\frac{1}{(1-xz)(1-x^2z)(1-x^3z)(1-x^4z)(1-x^5z)\text{ etc.}},$$

quae secundum potestates ipsius z evoluta praebeat hanc seriem

$$s=1+Az+Bz^2+Cz^3+Dz^4+Ez^5+\text{etc.},$$

eritque, ut supra (§ 6) notavimus, coefficiens A summa omnium terminorum huius seriei x, x^2, x^3, x^4, x^5 etc. seu $A = x^1 + x^2 + x^3 + x^4 + x^5 + x^6 +$ etc., quae est eadem series, quam in solutione praecedentis problematis pro littera A obtinuimus.

21. Deinde vero est B summa productorum ex binis terminis seriei A quadratis singulorum terminorum non exclusis. Hinc erit B summa omnium potestatum ipsius x, quarum exponentes sint aggregata duorum numerorum sive aequalium sive inaequalium; et cum eadem potestas hoc modo saepius resultare possit, ea unciam habebit numericam indicantem, quot ea potestas modis sit productum ex binis terminis seriei A seu quot variis modis eius exponens possit esse summa duorum numerorum tam aequalium quam inaequalium. Ex hoc fonte reperietur

$$B = x^2 + x^3 + 2x^4 + 2x^5 + 3x^6 + 3x^7 + 4x^8 + 4x^9 + \text{etc.},$$

cuius seriei quilibet coefficiens indicat, quot variis modis exponens potestatis ipsius x adiunctae in duas partes dispertiri possit. Hac igitur serie in infinitum continuata problematis propositi casus, quo partitio in duas partes requiritur, facile resolvitur.

22. Quantitas porro C, cum contineat omnia producta, quae oriuntur terminis ternis seriei A sive inaequalibus sive aequalibus invicem multiplicandis, constabit ex serie potestatum ipsius x, quarum exponentes sint summae trium numerorum integrorum affirmativorum. Atque eadem potestas x^n toties in serie C occurret, quoties eius exponens n ex tribus numeris sive aequalibus sive inaequalibus per additionem resultare potest. Erit autem

$$C = x^3 + x^4 + 2x^5 + 3x^6 + 4x^7 + 5x^8 + 7x^9 + 8x^{10} + 10x^{11} + \text{etc.},$$

cuius seriei quilibet coefficiens indicat, quot variis modis exponens potestatis ipsius x adiunctae in tres partes sive aequales sive inaequales dispertiri possit. Sic ex termino $8x^{10}$ colligitur numerum 10 octo modis diversis in tres partes secari posse, quae partitiones sunt

$$10 = 1 + 1 + 8, \qquad 10 = 2 + 2 + 6,$$
$$10 = 1 + 2 + 7, \qquad 10 = 2 + 3 + 5,$$
$$10 = 1 + 3 + 6, \qquad 10 = 2 + 4 + 4,$$
$$10 = 1 + 4 + 5, \qquad 10 = 3 + 3 + 4.$$

Ista igitur series C in infinitum continuata omnibus numeris in tres partes dispertiendis inserviet.

23. Simili modo quantitas D, cum contineat omnia producta ex quatuor terminis seriei $A = x + x^2 + x^3 + x^4 +$ etc. eiusdem termini repetitione non exclusa, constabit serie potestatum ipsius x, quarum exponentes sint aggregata quatuor numerorum sive aequalium sive inaequalium. In hac igitur serie quaelibet potestas ipsius x eiusmodi habebit coefficientem, qui indicet, quot variis modis eius exponens per additionem quatuor numerorum resultare possit. Reperietur autem hinc

$$D = x^4 + x^5 + 2x^6 + 3x^7 + 5x^8 + 6x^9 + 9x^{10} + 11x^{11} + \text{ etc.}$$

Haec igitur series in infinitum continuata ostendet, quot variis modis quilibet numerus in quatuor partes dispertiri possit. Sic ex termino $9x^{10}$ concluditur numerum 10 novem modis in quatuor partes dispertiri posse, quae partitiones sunt

$$10 = 1 + 1 + 1 + 7, \qquad 10 = 1 + 2 + 2 + 5,$$
$$10 = 1 + 1 + 2 + 6, \qquad 10 = 1 + 2 + 3 + 4,$$
$$10 = 1 + 1 + 3 + 5, \qquad 10 = 1 + 3 + 3 + 3,$$
$$10 = 1 + 1 + 4 + 4, \qquad 10 = 2 + 2 + 2 + 4,$$
$$10 = 2 + 2 + 3 + 3.$$

24. Hoc modo ulterius procedendo patebit litteram E fore seriem potestatum ipsius x ita comparatam, ut cuiusvis termini coefficiens indicet, quot variis modis exponens ipsius x in quinque partes dispertiri possit. Erit autem

$$E = x^5 + x^6 + 2x^7 + 3x^8 + 5x^9 + 7x^{10} + 10x^{11} + 13x^{12} + \text{etc.}$$

Pari modo valor litterae F erit series partitionibus in sex partes inserviens et litterarum G, H, I etc. valores pro partitionibus in partes septem, octo, novem etc. valebunt; erit autem

$$F = x^6 + x^7 + 2x^8 + 3x^9 + 5x^{10} + 7x^{11} + 11x^{12} + 14x^{13} + \text{etc.},$$
$$G = x^7 + x^8 + 2x^9 + 3x^{10} + 5x^{11} + 7x^{12} + 11x^{13} + 15x^{14} + \text{etc.}$$
etc.

Si hae series cum illis conferantur, quas in solutione superioris problematis pro iisdem litteris invenimus, mox patebit totum discrimen tantum in potestatibus ipsius x constare coefficientesque solos utrinque similiter procedere. Ne autem hic inductioni ullum locum concedamus, istam convenientiam sequenti demonstratione evincemus.

25. Consideremus ut supra duos valores ipsius s, qui sunt

$$s = 1 + Az + Bz^2 + Cz^3 + Dz^4 + Ez^5 + \text{etc.},$$
$$s = \frac{1}{(1-xz)(1-x^2z)(1-x^3z)(1-x^4z)(1-x^5z)\ \text{etc.}};$$

qui, si loco z ubique ponatur xz, abeant in t eritque

$$t = 1 + Axz + Bx^2z^2 + Cx^3z^3 + Dx^4z^4 + Ex^5z^5 + \text{etc.},$$
$$t = \frac{1}{(1-x^2z)(1-x^3z)(1-x^4z)(1-x^5z)\ \text{etc.}}.$$

Unde si posteriores ipsarum s et t valores invicem comparentur, mox patet esse $s = \frac{t}{1-xz}$ seu $t = (1-xz)s$; quae eadem relatio cum quoque inter priores litterarum s et t valores locum tenere debeat, erit

$$t = 1 + Axz + Bx^2z^2 + Cx^3z^3 + Cx^4z^4 + Ex^5z^5 + \text{etc.},$$
$$\begin{aligned}(1-xz)\,s = 1 &+ Az + Bz^2 + Cz^3 + Dz^4 + Ez^5 + \text{etc.}\\ &- xz - Axz^2 - Bxz^3 - Cxz^4 - Dxz^5 - \text{etc.}\end{aligned}$$

Unde per coaequationem terminorum homogeneorum invenitur

$$A = \frac{x}{1-x},$$
$$B = \frac{Ax}{1-xx} = \frac{x^2}{(1-x)(1-x^2)},$$
$$C = \frac{Bx}{1-x^3} = \frac{x^3}{(1-x)(1-x^2)(1-x^3)},$$
$$D = \frac{Cx}{1-x^4} = \frac{x^4}{(1-x)(1-x^2)(1-x^3)(1-x^4)}$$
etc.

26. Ex his formulis intelligitur istas series non solum quoque esse recurrentes uti superiores, sed etiam coefficientium utrinque eandem esse legem. Quare si neglectis numeratoribus ponatur

ut sit

$$\mathfrak{A} = \frac{1}{1-x}, \qquad A = \mathfrak{A}x,$$

$$\mathfrak{B} = \frac{1}{(1-x)(1-x^2)}, \qquad B = \mathfrak{B}x^2,$$

$$\mathfrak{C} = \frac{1}{(1-x)(1-x^2)(1-x^3)}, \qquad C = \mathfrak{C}x^3,$$

$$\mathfrak{D} = \frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)} \qquad D = \mathfrak{D}x^4$$

etc., etc.,

partitio cuiusque numeri in partes quotcunque sive aequales sive inaequales pendet a formatione serierum $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ etc., quae, uti ante observavimus, indicant, quot variis modis quivis numerus ex aliquot terminis initialibus huius seriei 1, 2, 3, 4, 5 etc. per additionem produci queat. Sic, cum sit $B = \mathfrak{B}x^2$, quivis numerus $n+2$ totidem modis in duas partes dispertiri potest, quot modis numerus n ex numeris 1 et 2 per additionem produci potest. Simili modo, cum sit $C = \mathfrak{C}x^3$, numerus $n+3$ tot modis in tres partes dispertietur, quot modis numerus n per additionem ex numeris 1, 2, 3 componi poterit. Atque generaliter numerus $n+m$ tot variis modis in m partes sive aequales sive inaequales dispertiri potest, quot modis numerus n ex numeris 1, 2, 3, ... m per additionem produci potest.

27. Pendet ergo et hoc problema a solutione quaestionis, qua quaeritur, quot variis modis datus numerus ex aliquot terminis initialibus huius seriei 1, 2, 3, 4 etc. per additionem resultare possit. Si igitur ut supra [§ 19] haec scribendi formula $n^{(m)}$ denotet numerum modorum, quibus numerus n ex numeris 1, 2, 3, ... m per additionem componi potest seu quibus numerus n in partes quotcunque distribui possit, quarum nulla maior sit numero m, huiusmodi characteribus et hoc problema propositum resolvi poterit. Scilicet $n^{(m)}$ indicabit, quot variis modis numerus $n+m$ in m partes sive aequales sive inaequales dispertiri possit. Hinc si quaeratur, quot modis numerus N in partes m sive aequales sive inaequales distribui possit, numerum modorum quaesitum indicabit haec formula $(N-m)^{(m)}$. Si igitur hoc problema cum

praecedente conferatur, perspicuum erit numerum $n+m$ totidem modis in m partes sive aequales sive inaequales distribui posse, quot modis numerus $n+\frac{m(m+1)}{2}$ in m partes inaequales dispertiri possit.

28. Solutio ergo amborum problematum a CEL. NAUDEO propositorum huc revocatur, ut definiatur, quot variis modis numerus quicunque n ex his numeris 1, 2, 3, ... m per additionem produci possit, seu ut investigetur valor characteris $n^{(m)}$. Quemadmodum ergo hoc novum problema ex formulis iam ante inventis commodissime resolvi queat, videamus. Ac primo quidem, si sit $m=1$, quia quilibet numerus unico modo ex meris unitatibus per additionem elici potest, erit

$$n^{(1)}=1,$$

quod idem prima formula $\mathfrak{A}=\frac{1}{1-x}$ seu series inde formata

$$\mathfrak{A}=1+x+x^2+x^3+x^4+x^5+\text{etc.}$$

manifesto indicat.

29. Quoniam series $\mathfrak{B}=\frac{1}{(1-x)(1-x^2)}$ indicat, quot modis quisque numerus ex numeris 1 et 2 per additionem formari possit, in hac serie potestatis x^n coefficiens erit $=n^{(2)}$; haec enim expressio assumta est ad significandum, quot modis numerus n ex numeris 1 et 2 per additionem oriri possit. Hinc igitur erit

$$\mathfrak{B}=1+1^{(2)}x+2^{(2)}x^2+3^{(2)}x^3+4^{(2)}x^4+5^{(2)}x^5+6^{(2)}x^6+\text{etc.}$$

atque ad similitudinem huius expressionis erit

$$\mathfrak{A}=1+1^{(1)}x+2^{(1)}x^2+3^{(1)}x^3+4^{(1)}x^4+5^{(1)}x^5+6^{(1)}x^6+\text{etc.}$$

Deinde vero cum sit $\mathfrak{A}=\frac{1}{1-x}$ et $\mathfrak{B}=\frac{1}{(1-x)(1-x^2)}$, erit $\mathfrak{A}=\mathfrak{B}(1-x^2)$, unde sequens inter has series relatio oritur

$$\begin{aligned}
\mathfrak{A} &= 1+1^{(1)}x+2^{(1)}x^2+3^{(1)}x^3+4^{(1)}x^4+5^{(1)}x^5+6^{(1)}x^6+\text{etc.},\\
\mathfrak{B} &= 1+1^{(2)}x+2^{(2)}x^2+3^{(2)}x^3+4^{(2)}x^4+5^{(2)}x^5+6^{(2)}x^6+\text{etc.}\\
-\mathfrak{B}x^2 &\qquad\qquad -x^2-1^{(2)}x^3-2^{(2)}x^4-3^{(2)}x^5-4^{(2)}x^6-\text{etc.}
\end{aligned}$$

Quodsi hinc coaequatio terminorum homogeneorum instituatur, erit

$$1^{(2)} = 1^{(1)}, \qquad 4^{(2)} = 4^{(1)} + 2^{(2)}, \qquad 7^{(2)} = 7^{(1)} + 5^{(2)},$$
$$2^{(2)} = 2^{(1)} + 1, \qquad 5^{(2)} = 5^{(1)} + 3^{(2)}, \qquad 8^{(2)} = 8^{(1)} + 6^{(2)},$$
$$3^{(2)} = 3^{(1)} + 1^{(2)}, \qquad 6^{(2)} = 6^{(1)} + 4^{(2)}, \qquad 9^{(2)} = 9^{(1)} + 7^{(2)}.$$

30. Generaliter ergo erit

$$n^{(2)} = n^{(1)} + (n-2)^{(2)}.$$

Cum igitur sit $n^{(1)} = 1$, erit $n^{(2)} = 1 + (n-2)^{(2)}$; sicque coefficientes seriei $\mathfrak{B}$ ita determinabuntur, ut quisque terminus ultimus aequalis sit antepenultimo unitate aucto. Seu cum seriei $\mathfrak{A}$ omnes coefficientes sint unitates, ex serie $\mathfrak{A}$ sequenti modo series $\mathfrak{B}$ formabitur:

$$\begin{array}{rcccccccccl}
\mathfrak{A} = 1 + x + & x^2 + & x^3 + & x^4 + & x^5 + & x^6 + & x^7 + & x^8 + & x^9 + \text{etc.} \\
& 1 & +1 & +2 & +2 & +3 & +3 & +4 & +4 & + \text{etc.} \\
\hline
\mathfrak{B} = 1 + x + & 2x^2 + & 2x^3 + & 3x^4 + & 3x^5 + & 4x^6 + & 4x^7 + & 5x^8 + & 5x^9 + \text{etc.}
\end{array}$$

Scilicet cum seriei $\mathfrak{B}$ duo termini initiales $1 + x$ constent, subscribantur ii sub terminis tertio et quarto seriei $\mathfrak{A}$ hincque per additionem orientur termini tertius et quartus seriei $\mathfrak{B}$, qui porro terminis quinto et sexto seriei $\mathfrak{A}$ subscripti et additi dabunt terminos quintum et sextum seriei $\mathfrak{B}$ hocque modo series $\mathfrak{B}$, quousque libuerit, facillime continuatur. Patet autem hinc esse $n^{(2)} = \frac{1}{2}\left(n \begin{smallmatrix} +1 \\ +2 \end{smallmatrix}\right)$; scilicet si n est numerus impar, erit $n^{(2)} = \frac{1}{2}(n+1)$, sin autem n sit numerus par, erit $n^{(2)} = \frac{1}{2}(n+2)$.

31. Cum porro sit $\mathfrak{C} = \frac{1}{(1-x)(1-x^2)(1-x^3)}$, erit $\mathfrak{B} = \mathfrak{C}(1-x^3)$, unde, cum seriei $\mathfrak{C}$ terminus generalis sit $n^{(3)}x^n$, sequens nascetur relatio inter series $\mathfrak{B}$ et $\mathfrak{C}$

$$\begin{aligned}
\mathfrak{B} &= 1 + 1^{(2)}x + 2^{(2)}x^2 + 3^{(2)}x^3 + 4^{(2)}x^4 + 5^{(2)}x^5 + 6^{(2)}x^6 + \text{etc.}, \\
\mathfrak{C} &= 1 + 1^{(3)}x + 2^{(3)}x^2 + 3^{(3)}x^3 + 4^{(3)}x^4 + 5^{(3)}x^5 + 6^{(3)}x^6 + \text{etc.} \\
-\mathfrak{C}x^3 & \qquad\qquad\qquad\qquad - x^3 - 1^{(3)}x^4 - 2^{(3)}x^5 - 3^{(3)}x^6 - \text{etc.}
\end{aligned}$$

Si iam hic aequatio inter terminos homogeneos instituatur, erit

$$1^{(3)} = 1^{(2)}, \qquad 4^{(3)} = 4^{(2)} + 1^{(3)}, \qquad 7^{(3)} = 7^{(2)} + 4^{(3)},$$
$$2^{(3)} = 2^{(2)}, \qquad 5^{(3)} = 5^{(2)} + 2^{(3)}, \qquad 8^{(3)} = 8^{(2)} + 5^{(3)},$$
$$3^{(3)} = 3^{(2)} + 1, \qquad 6^{(3)} = 6^{(2)} + 3^{(3)}, \qquad 9^{(3)} = 9^{(2)} + 6^{(3)}$$

et generaliter

$$n^{(3)} = n^{(2)} + (n-3)^{(3)}.$$

Series ergo $\mathfrak{C}$ ex serie $\mathfrak{B}$ suisque terminis antecedentibus sequenti modo facile formatur. Omittamus autem potestates ipsius x, quia totum negotium in coefficientibus versatur:

$$\begin{array}{rl} \mathfrak{B} = & 1+1+2+2+3+3+4+4+5+5+6+6+\text{etc.} \\ & \qquad\qquad\quad 1+1+2+3+4+5+7+8+10+\text{etc.} \\ \hline \mathfrak{C} = & 1+1+2+3+4+5+7+8+10+12+14+16+\text{etc.} \end{array}$$

Scilicet seriei $\mathfrak{B}$ subscribatur series $\mathfrak{C}$ initium sub termino quarto faciendo, et prouti hoc modo series $\mathfrak{C}$ per additionem oritur, ita quoque sub serie $\mathfrak{B}$ continuabitur.

32. Quia deinde est $\mathfrak{D} = \frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)}$, erit $\mathfrak{C} = \mathfrak{D}(1-x^4)$. Unde simili modo, quo hactenus sumus usi, reperietur:

$$1^{(4)} = 1^{(3)}, \qquad 4^{(4)} = 4^{(3)} + 1, \qquad 7^{(4)} = 7^{(3)} + 3^{(4)},$$
$$2^{(4)} = 2^{(3)}, \qquad 5^{(4)} = 5^{(3)} + 1^{(4)}, \qquad 8^{(4)} = 8^{(3)} + 4^{(4)},$$
$$3^{(4)} = 3^{(3)}, \qquad 6^{(4)} = 6^{(3)} + 2^{(4)}, \qquad 9^{(4)} = 9^{(3)} + 5^{(4)}$$

et generaliter

$$n^{(4)} = n^{(3)} + (n-4)^{(4)}.$$

Pari modo ulterius progrediendo colligetur fore

$$n^{(5)} = n^{(4)} + (n-5)^{(5)},$$
$$n^{(6)} = n^{(5)} + (n-6)^{(6)},$$
$$n^{(7)} = n^{(6)} + (n-7)^{(7)}$$
$$\text{etc.}$$

Generatim ergo hinc colligetur fore

$$n^{(m)} = n^{(m-1)} + (n-m)^{(m)},$$

ubi notandum est, si fuerit $n < m$, tum terminum $(n - m)^{(m)}$ prorsus evanescere, sin autem sit $n = m$, etiamsi sit $n - m = 0$, tamen terminum $(n - m)^{(m)}$ valere unitatem. Deinde si sit $n - m = 1$, quoque erit $(n - m)^{(m)} = 1$. Erit ergo perpetuo tam $0^{(m)} = 1$ quam $1^{(m)} = 1$ et $n^{(1)} = 1$.

33. His relationibus inter series 𝔄, 𝔅, ℭ, 𝔇 etc. notatis eae facillime formantur et, quousque libuerit, continuantur, quae operatio per hic adiunctum schematismum fiet manifesta:

	1	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}	x^{13}	x^{14}	x^{15} etc.
𝔄 =	1 +	1 +	1 +	1 +	1 +	1 +	1 +	1 +	1 +	1 +	1 +	1 +	1 +	1 +	1 +	1 + etc.
			1 +	1 +	2 +	2 +	3 +	3 +	4 +	4 +	5 +	5 +	6 +	6 +	7 +	7 + etc.
𝔅 =	1 +	1 +	2 +	2 +	3 +	3 +	4 +	4 +	5 +	5 +	6 +	6 +	7 +	7 +	8 +	8 + etc.
				1 +	1 +	2 +	3 +	4 +	5 +	7 +	8 +	10 +	12 +	14 +	16 +	19 + etc.
ℭ =	1 +	1 +	2 +	3 +	4 +	5 +	7 +	8 +	10 +	12 +	14 +	16 +	19 +	21 +	24 +	27 + etc.
					1 +	1 +	2 +	3 +	5 +	6 +	9 +	11 +	15 +	18 +	23 +	27 + etc.
𝔇 =	1 +	1 +	2 +	3 +	5 +	6 +	9 +	11 +	15 +	18 +	23 +	27 +	34 +	39 +	47 +	54 + etc.
						1 +	1 +	2 +	3 +	5 +	7 +	10 +	13 +	18 +	23 +	30 + etc.
𝔈 =	1 +	1 +	2 +	3 +	5 +	7 +	10 +	13 +	18 +	23 +	30 +	37 +	47 +	57 +	70 +	84 + etc.
							1 +	1 +	2 +	3 +	5 +	7 +	11 +	14 +	20 +	26 + etc.
𝔉 =	1 +	1 +	2 +	3 +	5 +	7 +	11 +	14 +	20 +	26 +	35 +	44 +	58 +	71 +	90 +	110 + etc.
								1 +	1 +	2 +	3 +	5 +	7 +	11 +	15 +	21 + etc.
𝔊 =	1 +	1 +	2 +	3 +	5 +	7 +	11 +	15 +	21 +	28 +	38 +	49 +	65 +	82 +	105 +	131 + etc.
									1 +	1 +	2 +	3 +	5 +	7 +	11 +	15 + etc.
ℌ =	1 +	1 +	2 +	3 +	5 +	7 +	11 +	15 +	22 +	29 +	40 +	52 +	70 +	89 +	116 +	146 + etc.
										1 +	1 +	2 +	3 +	5 +	7 +	11 + etc.
ℑ =	1 +	1 +	2 +	3 +	5 +	7 +	11 +	15 +	22 +	30 +	41 +	54 +	73 +	94 +	123 +	157 + etc.
											1 +	1 +	2 +	3 +	5 +	7 + etc.
𝔎 =	1 +	1 +	2 +	3 +	5 +	7 +	11 +	15 +	22 +	30 +	42 +	55 +	75 +	97 +	128 +	164 + etc.
												1 +	1 +	2 +	3 +	5 + etc.
𝔏 =	1 +	1 +	2 +	3 +	5 +	7 +	11 +	15 +	22 +	30 +	42 +	56 +	76 +	99 +	131 +	169 + etc.
													1 +	1 +	2 +	3 + etc.
𝔐 =	1 +	1 +	2 +	3 +	5 +	7 +	11 +	15 +	22 +	30 +	42 +	56 +	77 +	100 +	133 +	172 + etc.
														1 +	1 +	2 + etc.
𝔑 =	1 +	1 +	2 +	3 +	5 +	7 +	11 +	15 +	22 +	30 +	42 +	56 +	77 +	101 +	134 +	174 + etc.

etc.

34. Hoc modo tabula hic adiuncta[1]) per solam continuam additionem est constructa atque ratio constructionis tam est perspicua ex inspectione, ut ampliori explicatione non egeat. Ope huius tabulae igitur immediate resolvitur hoc problema, quo quaeritur, *quot variis modis datus numerus n ex his numeris* 1, 2, 3, ... m *per additionem produci possit.*

Sic si quaeratur, quot variis modis numerus 10 ex his numeris 1, 2 et 3 per additionem oriri possit, erit $n = 10$ et $m = 3$ atque ex tabula reperitur modorum numerus $= 14$, qui modi sunt

$10 = 1+1+1+1+1+1+1+1+1+1$,
$10 = 1+1+1+1+1+1+1+1+2$,
$10 = 1+1+1+1+1+1+1+3$,
$10 = 1+1+1+1+1+1+2+2$,
$10 = 1+1+1+1+1+2+3$,
$10 = 1+1+1+1+2+2+2$,
$10 = 1+1+1+1+3+3$,
$10 = 1+1+1+2+2+3$,
$10 = 1+1+2+2+2+2$,
$10 = 1+1+2+3+3$,
$10 = 1+2+2+2+3$,
$10 = 1+3+3+3$,
$10 = 2+2+2+2+2$,
$10 = 2+2+3+3$.

Si quaeratur, quot variis modis numerus 25 ex his numeris 1, 2, 3, 4, 5 per additionem produci possit, facto $n = 25$ et $m = 5$ reperietur ex tabula numerus modorum $= 377$.

Si quaeratur, quot variis modis numerus 50 ex his numeris 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 per additionem resultare possit, posito $n = 50$ et $m = 10$ invenitur modorum numerus $= 62740$.

Si vel numerus propositus vel numerus partium maior sit quam in tabula, tum nihilo minus casuum numerus ex tabula ope formularum supra inventarum colligi poterit. Uti si quaeratur, quot modis numerus 60 ex his numeris 1, 2, 3, ... 20 per additionem resultare possit, erit $n = 60$ et $m = 20$ quaeriturque valor formulae $60^{(20)}$. Est vero $60^{(20)} = 60^{(19)} + 40^{(20)}$, at $60^{(19)} = 60^{(18)} + 41^{(19)}$ porroque $60^{(18)} = 60^{(17)} + 42^{(18)}$ et $60^{(17)} = 60^{(16)} + 43^{(17)}$ sicque deinceps. Unde tandem erit

$$60^{(20)} = 40^{(20)} + 41^{(19)} + 42^{(18)} + 43^{(17)} + 44^{(16)} + \cdots + 59^{(1)},$$

qui numeri ex tabula collecti dant 791131; totque modis numerus 60 ex numeris 1, 2, 3, ... 20 per additionem elici potest.

1) Vide p. 290. In editione principe haec tabula nonnullos errores continet, qui omnes iam in *Comment. arithm.* correcti sunt. F. R.

35. Ope huius tabulae deinde ambo problemata Celeb. NAUDEI expedite resolvi possunt. Ac primo quidem si quaeratur, *quot variis modis datus numerus N in m partes inter se inaequales dispertiri possit,* hoc fiet, uti supra [§ 19] ostendimus, tot modis, quot unitates continentur in hac expressione $\left(N-\frac{m(m+1)}{2}\right)^{(m)}$, quam tabula indicat.

Usum igitur huius tabulae aliquot exemplis ostendamus.

I. *Quaeratur, quot variis modis numerus* 25 *in* 5 *partes inaequales dispertiri possit.*

Erit ergo hic $N=25$ et $m=5$, unde $\frac{m(m+1)}{2}=15$, et responsum continebit formula $10^{(5)}$, quae ex tabula est 30, ita ut partitio 30 modis institui possit.

II. *Quaeratur, quot variis modis numerus* 50 *in* 7 *partes inaequales dispertiri possit.*

Hic est $N=50$, $m=7$ et $N-\frac{m(m+1)}{2}=22$, unde numerus partitionum quaesitus est $22^{(7)}=522$.

III. *Quaeratur, quot variis modis numerus* 100 *in* 10 *partes inaequales dispertiri possit.*

Cum sit $N=100$ et $m=10$, erit $N-\frac{m(m+1)}{2}=45$ et numerus partitionum reperietur $45^{(10)}=33401$.

IV. *Quaeratur, quot diversis modis numerus* 256 *in* 20 *partes inaequales dispertiri possit.*

Ob $N=256$ et $m=20$ erit $N-\frac{m(m+1)}{2}=46$ et numerus partitionum fiet $46^{(20)}=96271$.

V. *Quaeratur, quot diversis modis numerus* 270 *in* 20 *partes inaequales dispertiri possit.*

Ob $N=270$ et $m=20$ erit $N-\frac{m(m+1)}{2}=60$ ideoque numerus partitionum quaesitus fit $60^{(20)}$, cuius valorem ante invenimus esse $=791131$. Tot ergo diversis modis numerus 270 in 20 partes inaequales dispertiri potest.

36. Simili modo ex tabula quoque alterum problema resolvetur, quo quaerebatur, *quot variis modis numerus N in m partes aequalitate partium non exclusa dispertiri possit.*

Supra [§ 27] enim ostendimus partitionum numerum quaesitum contineri in hac formula $(N-m)^{(m)}$, quem valorem ex tabula depromere licet. Quae solutio quo facilius intelligatur, aliquot exempla adiiciamus.

I. *Quaeratur, quot variis modis numerus 25 in 5 partes sive aequales sive inaequales dispertiri possit.*

Hic est $N=25$ et $m=5$, unde $N-m=20$, et partitionum numerus erit $20^{(5)}=192$.

II. *Quaeratur, quot variis modis numerus 50 in 7 partes sive aequales sive inaequales dispertiri possit.*

Ob $N=50$ et $m=7$ erit $N-m=43$ et partitionum numerus quaesitus fiet $43^{(7)}=8946$.

III. *Quaeratur, quot variis modis numerus 50 in 10 partes sive aequales sive inaequales dispertiri possit.*

Ob $N=50$ et $m=10$ erit $N-m=40$ et partitionum numerus erit $40^{(10)}=16928$.

IV. *Quaeratur, quot variis modis numerus 60 in 12 partes sive aequales sive inaequales dispertiri possit.*

Cum sit $N=60$ et $m=12$, erit $N-m=48$ et partitionum numerus quaesitus erit $48^{(12)}=74287$.

V. *Quaeratur, quot variis modis numerus 80 in 20 partes sive aequales sive inaequales dispertiri possit.*

Erit ergo $N=80$ et $m=20$, unde $N-m=60$, et partitionum numerus erit $60^{(20)}=791131$.

37. In seriebus horizontalibus, quas tabula exhibet, notatu digna est convenientia inter terminos initiales harum serierum, quae eo longius procedit, quo maior fuerit numerus m; sic series decima quinta quindecim suos terminos initiales cum omnibus seriebus sequentibus habet communes. Hinc inveniri poterit series, quae numero m in infinitum aucto respondet, quae ergo continebit valores huius formulae $n^{(\infty)}$, quae denotat, quot variis modis numerus n ex omnibus prorsus numeris integris per additionem produci possit. Haec ergo quaestio digna videtur, quae diligentius evolvatur. Cum $n^{(\infty)}$ complectatur omnes omnino partitiones numeri n pro quocunque partium

numero simul sumtas, erit $n^{(\sim)}$ aggregatum ex numeris partitionum in 1, 2, 3, 4, ... usque ad n partes sive aequales sive inaequales, quia numerus n in plures quam n partes secari nequit. Quamobrem erit

$$n^{(\sim)} = (n-1)^{(1)} + (n-2)^{(2)} + (n-3)^{(3)} + (n-4)^{(4)} + (n-5)^{(5)} + \cdots + (n-n)^{(n)},$$

in qua serie tam primus terminus $(n-1)^{(1)}$, qui denotat sectionem in unam partem, quam ultimus $(n-n)^{(n)}$, qui denotat sectionem in n partes, est unitas. Hinc igitur series numerorum $n^{(\sim)}$, quae in calce tabulae exhibetur, per additionem terminorum ex superioribus seriebus inveniri potest. Sic erit

$$6^{(\sim)} = 5^{(1)} + 4^{(2)} + 3^{(3)} + 2^{(4)} + 1^{(5)} + 0^{(6)} = 1 + 3 + 3 + 2 + 1 + 1 = 11,$$

qui numerus in infima tabulae serie sub numero 6 habetur.

38. Potest autem haec operatio contrahi ope lemmatis supra [§ 32] inventi $n^{(m)} = n^{(m-1)} + (n-m)^{(m)}$, unde fit $n^{(m)} - n^{(m-1)} = (n-m)^{(m)}$.

Cum enim sit

$$n^{(\sim)} = (n-1)^{(1)} + (n-2)^{(2)} + (n-3)^{(3)} + (n-4)^{(4)} + (n-5)^{(5)} + (n-6)^{(6)} + \text{etc.},$$

si ubique loco n scribatur $n-1$, erit

$$(n-1)^{(\sim)} = (n-1)^{(0)} + (n-2)^{(1)} + (n-3)^{(2)} + (n-4)^{(3)} + (n-5)^{(4)} + (n-6)^{(5)} + \text{etc.},$$

ubi ob uniformitatem praefigitur terminus $(n-1)^{(0)}$, cuius valor est $=0$. Si igitur inferior series a superiori subtrahatur, ope lemmatis prodibit

$$n^{(\sim)} - (n-1)^{(\sim)}$$
$$= (n-2)^{(1)} + (n-4)^{(2)} + (n-6)^{(3)} + (n-8)^{(4)} + (n-10)^{(5)} + (n-12)^{(6)} + \text{etc.}$$

sicque terminus quisque $n^{(\sim)}$ ope praecedentis $(n-1)^{(\sim)}$ per additionem duplo pauciorum terminorum quam ante invenitur. Erit ergo exempli gratia

$$12^{(\sim)} = 11^{(\sim)} + 10^{(1)} + 8^{(2)} + 6^{(3)} + 4^{(4)} + 2^{(5)} + 0^{(6)}$$

sive

$$12^{(\sim)} = 56 + 1 + 5 + 7 + 5 + 2 + 1 = 77,$$

qui numerus quoque pro valore ipsius $12^{(\sim)}$ in tabula reperitur.

39. Simili modo haec operatio ulterius contrahi potest; cum enim sit

$$n^{(\infty)}-(n-1)^{(\infty)}=(n-2)^{(1)}+(n-4)^{(2)}+(n-6)^{(3)}+(n-8)^{(4)}+(n-10)^{(5)}+\text{etc.},$$

si loco n ponamus $n-2$, habebimus

$$(n-2)^{(\infty)}-(n-3)^{(\infty)}$$
$$=(n-2)^{(0)}+(n-4)^{(1)}+(n-6)^{(2)}+(n-8)^{(3)}+(n-10)^{(4)}+\text{etc.},$$

ubi ob uniformitatem terminum $(n-2)^{(0)}=0$ praemittimus. Nunc hanc seriem a superiore subtrahendo ope lemmatis obtinebimus

$$n^{(\infty)}-(n-1)^{(\infty)}-(n-2)^{(\infty)}+(n-3)^{(\infty)}$$
$$=(n-3)^{(1)}+(n-6)^{(2)}+(n-9)^{(3)}+(n-12)^{(4)}+(n-15)^{(5)}+\text{etc.}$$

Haec ergo series si dicatur $=P$, erit

$$n^{(\infty)}=(n-1)^{(\infty)}+(n-2)^{(\infty)}-(n-3)^{(\infty)}+P.$$

In serie ergo quaesita ad definiendum terminum quemvis $n^{(\infty)}$ praeter valorem ipsius P nosse oportet ternos terminos praecedentes. Hoc modo procedendo tandem quantitas P evanescet et quilibet terminus istius seriei per solos terminos praecedentes definietur, quae est proprietas serierum recurrentium.

40. Hanc vero seriem revera esse recurrentem ex eius genesi est manifestum, cum oriatur ex evolutione huius fractionis

$$\frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)\text{ etc.}}.$$

Scala ergo relationis istius seriei habebitur, si iste denominator actu per multiplicationem evolvatur. Instituta autem hac multiplicatione denominator sequenti modo expressus invenietur:

$$1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-x^{40}+x^{51}+x^{57}-x^{70}-x^{77}+\text{etc.}^{1)}$$

Quae ipsius x potestates qualem teneant legem, ex ipsa formatione vix defi-

1) Vide notam p. 191. F. R.

niri posse videtur; interim tamen ex inspectione mox patet, alternatim binos terminos esse affirmativos et negativos. Neque minus exponentes ipsius x certam legem tenere observantur, unde eius terminus generalis colligitur esse $x^{n(3n\pm1):2}$. Scilicet nullae aliae potestates occurrunt, nisi quarum exponentes continentur in hac formula $\frac{3nn\pm n}{2}$, et ita quidem, ut potestates, quae ex numeris imparibus pro n assumtis oriuntur, habeant signum $-$, quae vero ex numeris paribus formantur, signum $+$.

41. Haec igitur forma nobis suppeditat scalam relationis seriei quaesitae, qua constat fore

$$n^{(\infty)}=(n-1)^{(\infty)}+(n-2)^{(\infty)}-(n-5)^{(\infty)}-(n-7)^{(\infty)}+(n-12)^{(\infty)}+(n-15)^{(\infty)}$$
$$-(n-22)^{(\infty)}-(n-26)^{(\infty)}+(n-35)^{(\infty)}+(n-40)^{(\infty)}-(n-51)^{(\infty)}-(n-57)^{(\infty)}+\text{etc.}$$

Hanc autem legem progressionis locum habere tentanti facile patebit. Sit enim $n=30$; reperietur fore

$$30^{(\infty)}=29^{(\infty)}+28^{(\infty)}-25^{(\infty)}-23^{(\infty)}+18^{(\infty)}+15^{(\infty)}-8^{(\infty)}-4^{(\infty)};$$

est enim his numeris ex tabula desumtis

$$5604=4565+3718-1958-1255+385+176-22-5.$$

Atque hoc modo ista series, quousque libuerit, continuari potest.

42. Quoniam vero series pro valore $m=20$ iam est formata, ex ea aliquanto facilius series quaesita pro valore $m=\infty$ erui poterit. Cum enim series $n^{(20)}$ formetur ex evolutione huius fractionis

$$\frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)\cdots(1-x^{20})},$$

series vero $n^{(\infty)}$ ex evolutione huius fractionis

$$\frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)\cdots(1-x^{\infty})},$$

manifestum est, si haec series multiplicetur per

$$(1-x^{21})(1-x^{22})(1-x^{23})(1-x^{24})(1-x^{25})\ \text{etc.}$$

seu per

$$\begin{aligned}
&1 - x^{21} - x^{22} - x^{23} - x^{24} - x^{25} - x^{26} - x^{27} - \text{etc.}\\
&+ x^{43} + x^{44} + 2x^{45} + 2x^{46} + 3x^{47} + 3x^{48} + 4x^{49} + 4x^{50} + \text{etc.}\\
&- x^{66} - x^{67} - 2x^{68} - 3x^{69} - 4x^{70} - 5x^{71} - 7x^{72} - 8x^{73} - 10x^{74} - \text{etc.}\\
&+ x^{90} + x^{91} + 2x^{92} + 3x^{93} + 5x^{94} + 6x^{95} + 9x^{96} + 11x^{97} + 15x^{98} + \text{etc.}\\
&- x^{115} - x^{116} - 2x^{117} - 3x^{118} - 5x^{119} - 7x^{120} - 10x^{121} - 13x^{122} - 18x^{123} - \text{etc.}\\
&\text{etc.,}
\end{aligned}$$

tum prodire debere priorem. Hinc concluditur fore

$$\begin{aligned}
n^{(20)} = n^{(\infty)} &- (n-21)^{(\infty)} - (n-22)^{(\infty)} - (n-23)^{(\infty)} - (n-24)^{(\infty)} - \text{etc.}\\
&+ (n-43)^{(\infty)} + (n-44)^{(\infty)} + 2(n-45)^{(\infty)} + 2(n-46)^{(\infty)} + 3(n-47)^{(\infty)} + \text{etc.}\\
&- (n-66)^{(\infty)} - (n-67)^{(\infty)} - 2(n-68)^{(\infty)} - 3(n-69)^{(\infty)} - 4(n-70)^{(\infty)} - \text{etc.}\\
&+ (n-90)^{(\infty)} + (n-91)^{(\infty)} + 2(n-92)^{(\infty)} + 3(n-93)^{(\infty)} + 5(n-94)^{(\infty)} + \text{etc.}\\
&- (n-115)^{(\infty)} - (n-116)^{(\infty)} - 2(n-117)^{(\infty)} - 3(n-118)^{(\infty)} - 5(n-119)^{(\infty)} - \text{etc.}\\
&\text{etc.,}
\end{aligned}$$

quarum serierum coefficientes procedunt secundum series superiores pro partitione numerorum in 2, 3, 4, 5, 6 etc. partes inservientes.

43. Denotet $\int (n-21)^{(\infty)}$ summam omnium terminorum seriei $n^{(\infty)}$, quae est

$$1 + 1 + 2 + 3 + 5 + 7 + 11 + 15 + 22 + 30 + \text{etc.}$$

usque ad terminum $(n-21)^{(\infty)}$ inclusive; similique modo sit generaliter $\int p^{(\infty)}$ summa omnium terminorum eiusdem seriei usque ad terminum $p^{(\infty)}$ inclusive; quae summae cum successive facile formentur, erit

$$\begin{aligned}
n^{(20)} = n^{(\infty)} &- \int (n-21)^{(\infty)} + \int (n-43)^{(\infty)} + \int (n-45)^{(\infty)} + \int (n-47)^{(\infty)} + \text{etc.}\\
&- \int (n-66)^{(\infty)} - \int (n-68)^{(\infty)} - \int (n-69)^{(\infty)} - \int (n-70)^{(\infty)} - \text{etc.}\\
&+ \int (n-90)^{(\infty)} + \int (n-92)^{(\infty)} + \int (n-93)^{(\infty)} + 2\int (n-94)^{(\infty)} + \text{etc.}\\
&\text{etc.}
\end{aligned}$$

Hincque adeo erit

$$n^{(\infty)} = n^{(20)} + \int(n-21)^{(\infty)} - \int(n-43)^{(\infty)} - \int(n-45)^{(\infty)} - \int(n-47)^{(\infty)} - \text{etc.}$$
$$+ \int(n-66)^{(\infty)} + \int(n-68)^{(\infty)} + \int(n-69)^{(\infty)} + \int(n-70)^{(\infty)} + \text{etc.}$$
$$- \int(n-90)^{(\infty)} - \int(n-92)^{(\infty)} - \int(n-93)^{(\infty)} - 2\int(n-94)^{(\infty)} - \text{etc.}$$

Huius formulae ope, nisi n sit numerus valde magnus, ex serie pro partitione in 20 partes inserviente ipsa series $n^{(\infty)}$ facile constituitur hocque modo ea in tabula constructa exhibetur, cum ubique excessus terminorum $n^{(\infty)}$ supra terminos $n^{(20)}$ sint assignati.

44. Hac igitur serie constructa proposito quocunque numero definiri poterit, quot omnino modis is in partes dispertiri possit. Sic patet numerum 10 omnino 42 modis ex additione resultare posse; atque numerus 59 tot modis, quot indicat iste numerus 831820, per additionem produci poterit. Sin autem numeri maiores proponantur, tum tabula hic exhibita ulterius continuari vel pro quovis casu numerus desideratus per praecepta hic tradita investigari debet. In his autem partitionibus aequalitas partium non excluditur. Unde novum oritur problema, *quo pro quovis numero proposito quaeritur omnium partitionum numerus in partes inter se inaequales*, quod problema resolvetur ope huius expressionis

$$(1+x)(1+x^2)(1+x^3)(1+x^4)(1+x^5)(1+x^6) \text{ etc.}$$

His enim factoribus in se invicem multiplicatis orietur series, in qua quilibet coefficiens ostendet, quot variis modis exponens ipsius x in partes inter se inaequales dispertiri possit.

45. Quodsi autem hoc productum actu evolvatur, reperietur haec series

$$1 + x + x^2 + 2x^3 + 2x^4 + 3x^5 + 4x^6 + 5x^7 + 6x^8 + 8x^9 + 10x^{10} + 12x^{11}$$
$$+ 15x^{12} + 18x^{13} + 22x^{14} + 27x^{15} + 32x^{16} + 38x^{17} + 46x^{18} + 54x^{19} + 64x^{20}$$
$$+ 76x^{21} + 89x^{22} + \text{etc.};$$

quae cum sit productum ex factoribus infinitis tam simplicem legem servantibus, omni attentione digna videtur. Ac primo quidem manifestum est

coefficientes horum terminorum plerumque esse pares et eos solum esse impares, qui sint cum eiusmodi ipsius x potestatibus coniuncti, quarum exponentes in hac forma $\frac{3nn \pm n}{2}$ contineantur; cuius phaenomeni eadem est ratio atque illius, quod circa exponentes eiusdem formae $\frac{3nn \pm n}{2}$ in evolutione producti $(1-x)(1-x^2)(1-x^3)(1-x^4)$ etc. observavimus. Cum autem sit

$$(1+x)(1+x^2)(1+x^3)(1+x^4) \text{ etc.} = \frac{(1-x^2)(1-x^4)(1-x^6)(1-x^8) \text{ etc.}}{(1-x)(1-x^2)(1-x^3)(1-x^4) \text{ etc.}},$$

apparet seriem ante inventam exprimi hac fractione

$$\frac{1-x^2-x^4+x^{10}+x^{14}-x^{24}-x^{30}+x^{44}+x^{52}-x^{70}-x^{80}+\text{ etc.}}{1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-x^{40}+\text{ etc.}},$$

unde ea ad modum serierum recurrentium formari poterit.

46. Facillime autem sine dubio haec series construitur ex ipsa eius indole, qua cuiuslibet termini coefficiens indicare debet, quot variis modis exponens ipsius x in partes inaequales dispertiri possit. Sit N coefficiens potestatis x^n in ista serie eritque

$$N = (n-1)^{(1)} + (n-3)^{(2)} + (n-6)^{(3)} + (n-10)^{(4)} + (n-15)^{(5)} + (n-21)^{(6)} + \text{etc.};$$

nam $(n-1)^{(1)} = 1$ indicat numerum n unico modo ex una parte constare, $(n-3)^{(2)}$ ostendit, quot modis numerus n in duas partes inaequales, $(n-6)^{(3)}$ ostendit, quot modis numerus n in tres partes inaequales distribui possit, et ita porro; unde et haec series ope tabulae datae, quousque libuerit, continuari potest. Ceterum hic notatu dignum est, si numeri partitionum in partes numero pares negative capiantur, hanc expressionem resultantem

$$(n-1)^{(1)} - (n-3)^{(2)} + (n-6)^{(3)} - (n-10)^{(4)} + (n-15)^{(5)} - (n-21)^{(6)} + \text{etc.}$$

semper esse $=0$, nisi fuerit n numerus in hac forma contentus $\frac{3zz \pm z}{2}$, sin autem n in hac forma contineatur, tum illius expressionis valorem esse vel $+1$ vel -1, prout z fuerit numerus vel impar vel par.[1])

1) Id quod perspicitur, si secundum paragraphum 40 evolutio

$$-(1-x)(1-x^2)(1-x^3)(1-x^4) \text{ etc.} = -1+x+x^2-x^5-x^7+x^{12}+x^{15}-\text{ etc.}$$

consideratur. F. R.

47. Quemadmodum hactenus omnes numeros integros ad partes constituendas admisimus, ita partium conditione limitanda numerus quaestionum in infinitum augeri posset; cui negotio, cum methodus certa ad huiusmodi quaestiones resolvendas sit tradita, non diutius immorabimur. Sufficiat ex praecedente insignem proprietatem partitionis in partes impares annotasse. Cum sit

$$(1+x)(1+x^2)(1+x^3)(1+x^4) \text{ etc.} = \frac{1}{(1-x)(1-x^3)(1-x^5)(1-x^7)(1-x^9) \text{ etc.}},$$

quae formula ex aequatione in § 45 exhibita sponte fluit, hinc sequitur quemvis numerum totidem modis ex numeris solis imparibus per additionem produci posse, quot modis idem numerus omnino in partes inter se inaequales dispertiri possit. Sic cum numerus 10 decem modis in partes inaequales dispertiri possit, qui modi sunt

$$\begin{array}{ll} 10 = 10, & 10 = 1+2+7, \\ 10 = 1+9, & 10 = 1+3+6, \\ 10 = 2+8, & 10 = 1+4+5, \\ 10 = 3+7, & 10 = 2+3+5, \\ 10 = 4+6, & 10 = 1+2+3+4, \end{array}$$

idem numerus 10 quoque decem modis ex solis numeris imparibus per additionem produci potest hoc modo

$$\begin{array}{ll} 10=1+1+1+1+1+1+1+1+1+1, & 10=1+3+3+3, \\ 10=1+1+1+1+1+1+1+3, & 10=1+1+1+1+3+3, \\ 10=1+1+1+1+1+5, & 10=1+1+3+5, \\ 10=1+1+1+7, & 10=3+7, \\ 10=1+9, & 10=5+5. \end{array}$$

48. Relictis autem his speculationibus progredior ad investigandum, quomodo quisque numerus ex terminis progressionis geometricae 1, 2, 4, 8, 16, 32 etc. per additionem formari possit.[1]) Ac primo quidem si istae partes

1) Vide notas 1—3 p. 258. F. R.

inter se debeant esse omnes inaequales, quaestio resolvetur per evolutionem huius expressionis

$$s = (1+x)(1+x^2)(1+x^4)(1+x^8)(1+x^{16})(1+x^{32}) \text{ etc.}$$

Multiplicatione enim actu instituta cuiusque termini coefficiens indicabit, quot modis exponens potestatis ipsius x adiunctae ex numeris progressionis geometricae 1, 2, 4, 8, 16 etc. per additionem produci possit. Cum igitur quivis numerus unico modo sic resolvi posse observatus sit, ostendendum est in hac serie omnes ipsius x potestates occurrere omniumque eundem esse coefficientem unitatem.

49. Ut hoc demonstremus, ponamus esse

$$s = 1 + \alpha x + \beta x^2 + \gamma x^3 + \delta x^4 + \varepsilon x^5 + \zeta x^6 + \eta x^7 + \theta x^8 + \text{etc.}$$

atque ad valores coefficientium $\alpha, \beta, \gamma, \delta$ etc. eruendos ponamus xx loco x sitque valor pro s hoc modo resultans $= t$; erit

$$t = (1+x^2)(1+x^4)(1+x^8)(1+x^{16})(1+x^{32}) \text{ etc.}$$

ideoque fiet $s = (1+x)t$. Qua relatione in seriebus considerata ob

$$t = 1 + \alpha x^2 + \beta x^4 + \gamma x^6 + \delta x^8 + \varepsilon x^{10} + \text{etc.}$$

habebitur

$$(1+x)t = 1 + x + \alpha x^2 + \alpha x^3 + \beta x^4 + \beta x^5 + \gamma x^6 + \gamma x^7 + \delta x^8 + \delta x^9 + \text{etc.};$$

quae cum aequalis esse debeat seriei s, comparatio coefficientium dabit

$$\begin{array}{llll} \alpha = 1, & \delta = \beta, & \eta = \gamma, & \varkappa = \varepsilon, \\ \beta = \alpha, & \varepsilon = \beta, & \theta = \delta, & \lambda = \varepsilon, \\ \gamma = \alpha, & \zeta = \gamma, & \iota = \delta, & \mu = \zeta \end{array}$$

etc.,

unde manifestum est singulos coefficientes esse unitati aequales ac propterea esse

$$s = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + \text{etc.} = \frac{1}{1-x};$$

quod idem per se perspicuum est, cum sit

$$(1-x)(1+x)(1+x^2)(1+x^4)(1+x^8)(1+x^{16}) \text{ etc.} = 1.$$

50. Sin autem quaeratur, quot variis modis quisque numerus ex terminis progressionis geometricae 1, 2, 4, 8, 16 etc. partium aequalitate non amplius sublata per additionem produci queat, solutio petenda erit ex evolutione huius fractionis

$$s = \frac{1}{(1-x)(1-x^2)(1-x^4)(1-x^8)(1-x^{16})(1-x^{32})\text{ etc.}};$$

hac enim in serie evoluta coefficiens cuiusque termini ostendet, quot variis modis exponens potestatis ipsius x adiunctae ex terminis progressionis geometricae propositae per additionem resultare possit. Ponamus xx loco x et valor ipsius s abeat in t; erit

$$t = \frac{1}{(1-x^2)(1-x^4)(1-x^8)(1-x^{16})\text{ etc.}} = (1-x)s;$$

sit igitur

$$s = 1 + \alpha x + \beta x^2 + \gamma x^3 + \delta x^4 + \varepsilon x^5 + \zeta x^6 + \eta x^7 + \theta x^8 + \iota x^9 + \text{etc.};$$

erit

$$\begin{aligned}(1-x)s &= 1 + \alpha x + \beta x^2 + \gamma x^3 + \delta x^4 + \varepsilon x^5 + \zeta x^6 + \eta x^7 + \theta x^8 + \iota x^9 + \text{etc.}\\ &\quad\; -1 \;\; -\alpha \;\; -\beta \;\; -\gamma \;\; -\delta \;\; -\varepsilon \;\; -\zeta \;\; -\eta \;\; -\theta \;\; -\text{etc.}\\ = t &= 1 \qquad + \alpha x^2 \qquad + \beta x^4 \qquad + \gamma x^6 \qquad + \delta x^8 \qquad + \text{etc.},\end{aligned}$$

unde ex aequalitate terminorum homogeneorum obtinebitur

$$\begin{array}{lll}\alpha = 1 \quad\;\; = 1, & \eta = \zeta \quad\;\; = 6, & \nu = \mu \quad\;\; = 20,\\ \beta = \alpha + \alpha = 2, & \theta = \eta + \delta = 10, & \xi = \nu + \eta = 26,\\ \gamma = \beta \quad\;\; = 2, & \iota = \theta \quad\;\; = 10, & o = \xi \quad\;\; = 26,\\ \delta = \gamma + \beta = 4, & \varkappa = \iota + \varepsilon = 14, & \pi = o + \theta = 36,\\ \varepsilon = \delta \quad\;\; = 4, & \lambda = \varkappa \quad\;\; = 14, & \varrho = \pi \quad\;\; = 36,\\ \zeta = \varepsilon + \gamma = 6, & \mu = \lambda + \zeta = 20, & \sigma = \varrho + \iota = 46\end{array}$$

etc.

51. Notatu digna est haec series, cum quod bini termini sint ubique aequales, tum quod ea facillime, quousque libuerit, continuetur. Ulterius autem continuata ita se habebit:

$$1+x+2x^2+2x^3+4x^4+4x^5+6x^6+6x^7+10x^8+10x^9+14x^{10}+14x^{11}$$
$$+20x^{12}+20x^{13}+26x^{14}+26x^{15}+36x^{16}+36x^{17}+46x^{18}+46x^{19}+60x^{20}+60x^{21}$$
$$+74x^{22}+74x^{23}+94x^{24}+94x^{25}+114x^{26}+114x^{27}+140x^{28}+140x^{29}+166x^{30}$$
$$+166x^{31}+202x^{32}+202x^{33}+238x^{34}+238x^{35}+284x^{36}+284x^{37}+\text{etc.}$$

Ex hac ergo serie patet numerum verbi gratia 30 centum sexaginta et sex modis ex terminis progressionis geometricae duplae per additionem produci posse. Ceterum attendenti facile patebit legem huius progressionis nullo modo per terminum generalem exprimi posse, cum revera sit series recurrens, cuius scala relationis in infinitum extendatur. Dabit autem hoc productum infinitum

$$(1-x)(1-x^2)(1-x^4)(1-x^8)(1-x^{16})(1-x^{32})\text{ etc.},$$

si evolvatur, scalam relationis. Ad quam inveniendam ponatur hoc productum $=p$, quod abeat in q, si loco x ponatur x^2, eritque

$$q=(1-x^2)(1-x^4)(1-x^8)(1-x^{16})\text{ etc.}=\frac{p}{1-x}$$

seu $p=(1-x)q$. Statuatur ergo

$$p=1+\alpha x+\beta x^2+\gamma x^3+\delta x^4+\varepsilon x^5+\zeta x^6+\eta x^7+\theta x^8+\iota x^9+\varkappa x^{10}+\text{etc.},$$

eritque

$$(1-x)q=1-x+\alpha x^2-\alpha x^3+\beta x^4-\beta x^5+\gamma x^6-\gamma x^7+\delta x^8-\delta x^9+\varepsilon x^{10}-\text{etc.},$$

unde per coaequationem terminorum similium obtinetur

$\alpha=-1=-1,$	$\theta=\delta=-1,$	$o=-\eta=+1,$
$\beta=\alpha=-1,$	$\iota=-\delta=+1,$	$\pi=\theta=-1,$
$\gamma=-\alpha=+1,$	$\varkappa=\varepsilon=+1,$	$\varrho=-\theta=+1,$
$\delta=\beta=-1,$	$\lambda=-\varepsilon=-1,$	$\sigma=\iota=+1,$
$\varepsilon=-\beta=+1,$	$\mu=\zeta=+1,$	$\tau=-\iota=-1,$
$\zeta=\gamma=+1,$	$\nu=-\zeta=-1,$	$\upsilon=\varkappa=+1,$
$\eta=-\gamma=-1,$	$\xi=\eta=-1,$	$\varphi=-\varkappa=-1$

etc.

52. Coefficientes ergo seriei p, quae ex evolutione huius producti

$$(1-x)(1-x^2)(1-x^4)(1-x^8)(1-x^{16})(1-x^{32})\text{ etc.}$$

nascitur, omnes sunt vel $+1$ vel -1 neque tamen legem obtinent solito more assignabilem; erit enim

$$\begin{aligned}p = 1 &- x^1 - x^2 + x^3 - x^4 + x^5 + x^6 - x^7 - x^8 + x^9 + x^{10} - x^{11} + x^{12} - x^{13} - x^{14}\\ &+ x^{15} - x^{16} + x^{17} + x^{18} - x^{19} + x^{20} - x^{21} - x^{22} + x^{23} + x^{24} - x^{25} - x^{26} + x^{27} - x^{28}\\ &+ x^{29} + x^{30} - x^{31} - x^{32} + x^{33} + x^{34} - x^{35} + x^{36} - x^{37} - x^{38} + x^{39} + x^{40} - x^{41} - x^{42}\\ &+ x^{43} - x^{44} + \text{etc.},\end{aligned}$$

ubi notandum est quamlibet potestatem exponentis imparis x^{2n+1} contrarium habere signum ei, quod habet potestas x^{2n}, huiusque signum perpetuo convenire cum signo potestatis x^n; unde cuiusvis potestatis signum facile assignabitur. Uti si quaeratur signum potestatis huius x^{1745}, erit respectu ad sola signa habito

$$\begin{aligned}x^{1745} &= -x^{1744} = -x^{872} = -x^{436} = -x^{218} = -x^{109} = +x^{108} = +x^{54} = +x^{27}\\ &= -x^{26} = -x^{13} = +x^{12} = +x^6 = +x^3 = -x^2 = -x^1;\end{aligned}$$

signum ergo potestatis x^{1745} contrarium est signo potestatis x^1; quod cum sit $-$, erit id $+$.[1])

1) Secundum EULERI consuetudines etiam alibi notatas (cf. ex. gr. notam p. 3 libri, qui inscribitur *Vollständige Anleitung zur Algebra*, LEONHARDI EULERI *Opera omnia*, series I vol. 1) ex hoc exemplo 1745 concludere licet EULERUM has investigationes iam a. 1745 conscripsisse. F. R.

Tabula indicans, quot variis modis quilibet numerus n ex numeris 1, 2, 3, 4, ... m per additionem produci possit, seu exhibens valores formulae $n^{(m)}$.

	Valores numeri n															
m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	$\overset{0}{1}$	$\overset{1}{2}$	$\overset{1}{2}$	$\overset{2}{3}$	$\overset{2}{3}$	$\overset{3}{4}$	$\overset{3}{4}$	$\overset{4}{5}$	$\overset{4}{5}$	$\overset{5}{6}$	$\overset{5}{6}$	$\overset{6}{7}$	$\overset{6}{7}$	$\overset{7}{8}$	$\overset{7}{8}$
3	1	1	2	$\overset{1}{3}$	$\overset{1}{4}$	$\overset{2}{5}$	$\overset{3}{7}$	$\overset{4}{8}$	$\overset{5}{10}$	$\overset{7}{12}$	$\overset{8}{14}$	$\overset{10}{16}$	$\overset{12}{19}$	$\overset{14}{21}$	$\overset{16}{24}$	$\overset{19}{27}$
4	1	1	2	3	$\overset{1}{5}$	$\overset{1}{6}$	$\overset{2}{9}$	$\overset{3}{11}$	$\overset{5}{15}$	$\overset{6}{18}$	$\overset{9}{23}$	$\overset{11}{27}$	$\overset{15}{34}$	$\overset{18}{39}$	$\overset{23}{47}$	$\overset{27}{54}$
5	1	1	2	3	5	$\overset{1}{7}$	$\overset{1}{10}$	$\overset{2}{13}$	$\overset{3}{18}$	$\overset{5}{23}$	$\overset{7}{30}$	$\overset{10}{37}$	$\overset{13}{47}$	$\overset{18}{57}$	$\overset{23}{70}$	$\overset{30}{84}$
6	1	1	2	3	5	7	$\overset{1}{11}$	$\overset{1}{14}$	$\overset{2}{20}$	$\overset{3}{26}$	$\overset{5}{35}$	$\overset{7}{44}$	$\overset{11}{58}$	$\overset{14}{71}$	$\overset{20}{90}$	$\overset{26}{110}$
7	1	1	2	3	5	7	11	$\overset{1}{15}$	$\overset{1}{21}$	$\overset{2}{28}$	$\overset{3}{38}$	$\overset{5}{49}$	$\overset{7}{65}$	$\overset{11}{82}$	$\overset{15}{105}$	$\overset{21}{131}$
8	1	1	2	3	5	7	11	15	$\overset{1}{22}$	$\overset{1}{29}$	$\overset{2}{40}$	$\overset{3}{52}$	$\overset{5}{70}$	$\overset{7}{89}$	$\overset{11}{116}$	$\overset{15}{146}$
9	1	1	2	3	5	7	11	15	22	$\overset{1}{30}$	$\overset{1}{41}$	$\overset{2}{54}$	$\overset{3}{73}$	$\overset{5}{94}$	$\overset{7}{123}$	$\overset{11}{157}$
10	1	1	2	3	5	7	11	15	22	30	$\overset{1}{42}$	$\overset{1}{55}$	$\overset{2}{75}$	$\overset{3}{97}$	$\overset{5}{128}$	$\overset{7}{164}$
11	1	1	2	3	5	7	11	15	22	30	42	$\overset{1}{56}$	$\overset{1}{76}$	$\overset{2}{99}$	$\overset{3}{131}$	$\overset{5}{169}$
12	1	1	2	3	5	7	11	15	22	30	42	56	$\overset{1}{77}$	$\overset{1}{100}$	$\overset{2}{133}$	$\overset{3}{172}$
13	1	1	2	3	5	7	11	15	22	30	42	56	77	$\overset{1}{101}$	$\overset{1}{134}$	$\overset{2}{174}$
14	1	1	2	3	5	7	11	15	22	30	42	56	77	101	$\overset{1}{135}$	$\overset{1}{175}$
15	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	$\overset{1}{176}$
16	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176
17	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176
18	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176
19	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176
20	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176
∞	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176

m	16	17	18	19	20	21	22	23	24	25	26
1	1	1	1	1	1	1	1	1	1	1	1
2	8 9	8 9	9 10	9 10	10 11	10 11	11 12	11 12	12 13	12 13	13 14
3	21 30	24 33	27 37	30 40	33 44	37 48	40 52	44 56	48 61	52 65	56 70
4	34 64	39 72	47 84	54 94	64 108	72 120	84 136	94 150	108 169	120 185	136 206
5	37 101	47 119	57 141	70 164	84 192	101 221	119 255	141 291	164 333	192 377	221 427
6	35 136	44 163	58 199	71 235	90 282	110 331	136 391	163 454	199 532	235 612	282 709
7	28 164	38 201	49 248	65 300	82 364	105 436	131 522	164 618	201 733	248 860	300 1009
8	22 186	29 230	40 288	52 352	70 434	89 525	116 638	146 764	186 919	230 1090	288 1297
9	15 201	22 252	30 318	41 393	54 488	73 598	94 732	123 887	157 1076	201 1291	252 1549
10	11 212	15 267	22 340	30 423	42 530	55 653	75 807	97 984	128 1204	164 1455	212 1761
11	7 219	11 278	15 355	22 445	30 560	42 695	56 863	76 1060	99 1303	131 1586	169 1930
12	5 224	7 285	11 366	15 460	22 582	30 725	42 905	56 1116	77 1380	100 1686	133 2063
13	3 227	5 290	7 373	11 471	15 597	22 747	30 935	42 1158	56 1436	77 1763	101 2164
14	2 229	3 293	5 378	7 478	11 608	15 762	22 957	30 1188	42 1478	56 1819	77 2241
15	1 230	2 295	3 381	5 483	7 615	11 773	15 972	22 1210	30 1508	42 1861	56 2297
16	1 231	1 296	2 383	3 486	5 620	7 780	11 983	15 1225	22 1530	30 1891	42 2339
17	231	1 297	1 384	2 488	3 623	5 785	7 990	11 1236	15 1545	22 1913	30 2369
18	231	297	1 385	1 489	2 625	3 788	5 995	7 1243	11 1556	15 1928	22 2391
19	231	297	385	1 490	1 626	2 790	3 998	5 1248	7 1563	11 1939	15 2406
20	231	297	385	490	1 627	1 791	2 1000	3 1251	5 1568	7 1946	11 2417
∞	231	297	385	490	627	1 792	2 1002	4 1255	7 1575	12 1958	19 2436

m	27	28	29	30	31	32	33	34	35	36	37
1	1	1	1	1	1	1	1	1	1	1	1
2	13 14	14 15	14 15	15 16	15 16	16 17	16 17	17 18	17 18	18 19	18 19
3	61 75	65 80	70 85	75 91	80 96	85 102	91 108	96 114	102 120	108 127	114 133
4	150 225	169 249	185 270	206 297	225 321	249 351	270 378	297 411	321 441	351 478	378 511
5	255 480	291 540	333 603	377 674	427 748	480 831	540 918	603 1014	674 1115	748 1226	831 1342
6	331 811	391 931	454 1057	532 1206	612 1360	709 1540	811 1729	931 1945	1057 2172	1206 2432	1360 2702
7	364 1175	436 1367	522 1579	618 1824	733 2093	860 2400	1009 2738	1175 3120	1367 3539	1579 4011	1824 4526
8	352 1527	434 1801	525 2104	638 2462	764 2857	919 3319	1090 3828	1297 4417	1527 5066	1801 5812	2104 6630
9	318 1845	393 2194	488 2592	598 3060	732 3589	887 4206	1076 4904	1291 5708	1549 6615	1845 7657	2194 8824
10	267 2112	340 2534	423 3015	530 3590	653 4242	807 5013	984 5888	1204 6912	1455 8070	1761 9418	2112 10936
11	219 2331	278 2812	355 3370	445 4035	560 4802	695 5708	863 6751	1060 7972	1303 9373	1586 11004	1930 12866
12	172 2503	224 3036	285 3655	366 4401	460 5262	582 6290	725 7476	905 8877	1116 10489	1380 12384	1686 14552
13	134 2637	174 3210	227 3882	290 4691	373 5635	471 6761	597 8073	747 9624	935 11424	1158 13542	1436 15988
14	101 2738	135 3345	175 4057	229 4920	293 5928	378 7139	478 8551	608 10232	762 12186	957 14499	1188 17176
15	77 2815	101 3446	135 4192	176 5096	230 6158	295 7434	381 8932	483 10715	615 12801	773 15272	972 18148
16	56 2871	77 3523	101 4293	135 5231	176 6334	231 7665	296 9228	383 11098	486 13287	620 15892	780 18928
17	42 2913	56 3579	77 4370	101 5332	135 6469	176 7841	231 9459	297 11395	384 13671	488 16380	623 19551
18	30 2943	42 3621	56 4426	77 5409	101 6570	135 7976	176 9635	231 11626	297 13968	385 16765	489 20040
19	22 2965	30 3651	42 4468	56 5465	77 6647	101 8077	135 9770	176 11802	231 14199	297 17062	385 20425
20	15 2980	22 3673	30 4498	42 5507	56 6703	77 8154	101 9871	135 11937	176 14375	231 17293	297 20722
∞	30 3010	45 3718	67 4565	97 5604	139 6842	195 8349	272 10143	373 12310	508 14883	684 17977	915 21637

m	38	39	40	41	42	43	44	45	46	47	48
1	1	1	1	1	1	1	1	1	1	1	1
2	19 20	19 20	20 21	20 21	21 22	21 22	22 23	22 23	23 24	23 24	24 25
3	120 140	127 147	133 154	140 161	147 169	154 176	161 184	169 192	176 200	184 208	192 217
4	411 551	441 588	478 632	511 672	551 720	588 764	632 816	672 864	720 920	764 972	816 1033
5	918 1469	1014 1602	1115 1747	1226 1898	1342 2062	1469 2233	1602 2418	1747 2611	1898 2818	2062 3034	2233 3266
6	1540 3009	1729 3331	1945 3692	2172 4070	2432 4494	2702 4935	3009 5427	3331 5942	3692 6510	4070 7104	4494 7760
7	2093 5102	2400 5731	2738 6430	3120 7190	3539 8033	4011 8946	4526 9953	5102 11044	5731 12241	6430 13534	7190 14950
8	2462 7564	2857 8588	3319 9749	3828 11018	4417 12450	5066 14012	5812 15765	6630 17674	7564 19805	8588 22122	9749 24699
9	2592 10156	3060 11648	3589 13338	4206 15224	4904 17354	5708 19720	6615 22380	7657 25331	8824 28629	10156 32278	11648 36347
10	2534 12690	3015 14663	3590 16928	4242 19466	5013 22367	5888 25608	6912 29292	8070 33401	9418 38047	10936 43214	12690 49037
11	2331 15021	2812 17475	3370 20298	4035 23501	4802 27169	5708 31316	6751 36043	7972 41373	9373 47420	11004 54218	12866 61903
12	2068 17084	2503 19978	3036 23334	3655 27156	4401 31570	5262 36578	6290 42333	7476 48849	8877 56297	10489 64707	12384 74287
13	1768 18847	2164 22142	2637 25971	3210 30366	3882 35452	4691 41269	5635 47968	6761 55610	8073 64370	9624 74331	11424 85711
14	1478 20325	1819 23961	2241 28212	2738 33104	3345 38797	4057 45326	4920 52888	5928 61538	7139 71509	8551 82882	10232 95943
15	1210 21535	1508 25469	1861 30073	2297 35401	2815 41612	3446 48772	4192 57080	5096 66634	6158 77667	7434 90316	8932 104875
16	983 22518	1225 26694	1530 31603	1891 37292	2339 43951	2871 51643	3523 60603	4293 70927	5231 82898	6334 96650	7665 112540
17	785 23303	990 27684	1236 32839	1545 38837	1913 45864	2369 54012	2913 63516	3579 74506	4370 87268	5332 101982	6469 119009
18	625 23928	788 28472	995 33834	1243 40080	1556 47420	1928 55940	2391 65907	2943 77449	3621 90889	4426 106408	5409 124418
19	490 24418	626 29098	790 34624	998 41078	1248 48668	1563 57503	1939 67846	2406 79855	2965 93854	3651 110059	4468 128886
20	385 24803	490 29588	627 35251	791 41869	1000 49668	1251 58754	1568 69414	1946 81801	2417 96271	2980 113039	3673 132559
∞	1212 26015	1597 31185	2087 37338	2714 44583	3506 53174	4507 63261	5761 75175	7333 89134	9287 105558	11715 124754	14714 147273

m	49	50	51	52	53	54	55	56	57	58	59
1	1	1	1	1	1	1	1	1	1	1	1
2	24 25	25 26	25 26	26 27	26 27	27 28	27 28	28 29	28 29	29 30	29 30
3	200 225	208 234	217 243	225 252	234 261	243 271	252 280	261 290	271 300	280 310	290 320
4	864 1089	920 1154	972 1215	1033 1285	1089 1350	1154 1425	1215 1495	1285 1575	1350 1650	1425 1735	1495 1815
5	2418 3507	2611 3765	2818 4033	3034 4319	3266 4616	3507 4932	3765 5260	4033 5608	4319 5969	4616 6351	4932 6747
6	4935 8442	5427 9192	5942 9975	6510 10829	7104 11720	7760 12692	8442 13702	9192 14800	9975 15944	10829 17180	11720 18467
7	8033 16475	8946 18138	9958 19928	11044 21873	12241 23961	13534 26226	14950 28652	16475 31275	18138 34082	19928 37108	21873 40340
8	11018 27493	12450 30588	14012 33940	15765 37638	17674 41635	19805 46031	22122 50774	24699 55974	27493 61575	30588 67696	33940 74280
9	13338 40831	15224 45812	17354 51294	19720 57358	22380 64015	25331 71362	28629 79403	32278 88252	36347 97922	40831 108527	45812 120092
10	14663 55494	16928 62740	19466 70760	22367 79725	25608 89623	29292 100654	33401 112804	38047 126299	43214 141136	49037 157564	55494 175586
11	15021 70515	17475 80215	20298 91058	23501 103226	27169 116792	31316 131970	36043 148847	41373 167672	47420 188556	54218 211782	61908 237489
12	14552 85067	17084 97299	19978 111036	23334 126560	27156 143948	31570 163540	36578 185425	42333 210005	48849 237405	56297 268079	64707 302196
13	13542 98609	15988 113287	18847 129883	22142 148702	25971 169919	30366 193906	35452 220877	41269 251274	47968 285373	55610 323689	64370 366566
14	12186 110795	14499 127786	17176 147059	20325 169027	23961 193880	28212 222118	33104 253981	38797 290071	45326 330699	52888 376577	61538 428104
15	10715 121510	12801 140587	15272 162331	18148 187175	21535 215415	25469 247587	30073 284054	35401 325472	41612 372311	48772 425349	57080 485184
16	9228 130738	11098 151685	13287 175618	15892 203067	18928 234343	22518 270105	26694 310748	31603 357075	37292 409603	43951 469300	51643 536827
17	7841 138579	9459 161144	11395 187013	13671 216738	16380 250723	19551 289656	23303 334051	27684 384759	32839 442442	38837 508137	45864 582691
18	6570 145149	7976 169120	9635 196648	11626 228364	13968 264691	16765 306421	20040 354091	23928 408687	28472 470914	33834 541971	40080 622771
19	5465 150614	6647 175767	8077 204725	9770 238134	11802 276493	14199 320620	17062 371153	20425 429112	24418 495332	29098 571069	34624 657395
20	4498 155112	5507 181274	6703 211428	8154 246288	9871 286364	11937 332557	14375 385528	17293 446405	20722 516054	24803 595872	29588 686983
∞	18413 173525	22952 204226	28515 239943	35301 281589	43567 329931	53598 386155	65748 451276	80418 526823	98100 614154	119348 715220	144837 831820

DE NUMERIS QUI SUNT AGGREGATA DUORUM QUADRATORUM[1])

Commentatio 228 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 4 (1752/3), 1758, p. 3—40
Summarium ibidem p. 5—8

SUMMARIUM

Non frustra est, quod veteres Mathematici, uti ex scriptis EUCLIDIS ac DIOPHANTI liquet, summo studio numerorum indolem scrutati proprietatibus eorum haud mediocriter delectati sunt. Praeterito etiam saeculo primi ordinis Geometrae plurimum studii in exploranda numerorum natura consumserunt, inter quos FERMATIUS Senator Tolosanus ita eminuit, ut eius sagacitatem etiamnunc nemo sit assecutus. Mos tunc invaluerat veritates, quas quisque investigasset, nude potius ad ceterorum ingenia exercenda proponere, quam demonstrationes docendi causa indicare; quo factum est, ut sublimes FERMATII meditationes in hoc genere adhuc hodie magis miremur quam cognoscamus, propterea quod post eius obitum scripta, quibus earum demonstrationes continebantur, temporis iniuria maximo huius scientiae damno interierunt.

Praestantissimus itaque Auctor huius dissertationis haud inutiliter operam suam collocare censendus est, dum huiusmodi deperditas demonstrationes FERMATIANAS restaurare conatur, etiamsi nostro quidem aevo hoc studium, quod in numerorum natura investiganda consumitur, plane derelictum atque adeo a plerisque spretum videatur. Quanquam enim hoc quidem tempore Mathematici in cultura Analyseos sublimioris et partibus Matheseos applicatae, quae veteribus inaccessae fuerunt, potissimum elaborare solent, nulla tamen veritas prorsus sterilis et omni usu destituta videtur. Quin potius numerorum proprietates plerumque multo maiorem sagacitatem et ingenii vim postulant, quod vel ex eo colligere

1) Vide ad hanc Commentationem epistolam ab EULERO d. 6. Maii 1747 ad CHR. GOLDBACH scriptam, *Correspondance math. et phys. publiée par P. H. FUSS*, St.-Pétersbourg 1843, t. I, p. 413; *LEONHARDI EULERI Opera omnia*, series III. F. R.

licet, quod in reliquis Matheseos partibus vix ulla cognoscatur veritas, cuius demonstratio non ante iam fuerit perspecta, cum contra plurimae habeantur numerorum proprietates, quarum veritatem adhuc sine demonstratione admittere cogimur auctoritate potissimum FERMATII inducti, qui se eas demonstrasse palam est professus.

Ad hoc genus referendae sunt plures insignes proprietates numerorum, qui sunt binorum quadratorum aggregata, quarum demonstrationes Cel. Auctor in hac dissertatione proponit. De his numeris, siquidem bina quadrata eos componentia fuerint inter se prima seu communem divisorem non admittant, id prorsus est singulare, quod alios divisores non agnoscant, nisi qui ipsi eiusdem sint indolis, binorum scilicet quadratorum summae, cuius rei demonstratio haud parum ardua hic suppeditatur. Deinde cum omnes huius generis numeri, si fuerint primi, unitate minuti per quaternarium sint divisibiles sive in hac forma $4n+1$ contineantur, memorabile est vicissim omnes numeros primos huius formae $4n+1$ simul esse summas duorum quadratorum, cuius demonstrationis autem se nondum compotem esse factum Cel. Auctor ingenue fatetur, etiamsi eius veritatem extra dubium collocaverit; in quo insigne conspicitur specimen etiam in mathematicis eiusmodi dari veritates, quas sine perfecta demonstratione credere cogimur. In sequenti volumine Commentariorum nostrorum plena eiusdem demonstratio apparebit, qua omnia, quae hinc derivantur, penitus confirmabuntur.[1])

Hic ex ista proprietate egregiam deduxit methodum eamque satis facilem explorandi, utrum numerus huius formae $4n+1$, quantumvis fuerit magnus, primus sit necne. Totum negotium huc redit, ut exploretur, utrum talis numerus propositus in summam duorum quadratorum resolvi queat an minus; ubi tres casus sunt perpendendi. Primo si numerus propositus nullo prorsus modo in duo quadrata sit resolubilis, certum est eum non esse primum, sed duos ad minimum factores habere formae $4m-1$; secundo si unico modo in duo quadrata fuerit resolubilis eaque sint prima inter se, hoc certum est indicium numerum propositum esse primum; tertio si is plus uno modo in duo quadrata discerpi queat, necessario erit compositus eiusque divisores inde assignari possunt. Vulgo autem iudicium, utrum numerus propositus sit primus necne, haud parum molestiae creare solet, si is centena millia superet. Ad hunc enim terminum usque habentur tabulae numerorum primorum passim obviae atque adeo sinicis characteribus exaratae.[2]) Pro maioribus autem numeris adhuc alia via non patuit, nisi ut divisio per omnes numeros primos usque ad radicem quadratam numeri propositi tentetur. Nunc autem, dum numerus propositus in forma $4n+1$ contineatur, totum negotium multo minore labore absolvitur, cuius plura ad calcem huius tractationis extant specimina, quod eo magis notatu dignum videtur, quod nulla operatio per divisores instituatur.

1) Vide Commentationem 241 huius voluminis. F. R.
2) Vide notam 3 p. 104. F. R.

1. Naturam numerorum pluribus modis scrutari solent Arithmetici, dum eorum originem vel per additionem vel per multiplicationem repraesentant. Prioris generis sine dubio simplicissima est compositio ex unitatibus, qua omnes numeri integri per aggregationem unitatum oriri concipiuntur. Tum numeri quoque ita considerari possunt, prouti ex additione duorum pluriumve aliorum numerorum integrorum nascuntur, quo pertinet problema de partitione numerorum, cuius solutionem aliquot abhinc annis exposui[1]), in quo quaeritur, quot variis modis quilibet numerus propositus per additionem duorum pluriumve numerorum minorum resultare possit. Hic autem constitui eam numerorum compositionem perpendere, qua per additionem duorum quadratorum prodeunt; et cum hoc modo non omnes numeri oriantur, quoniam ingens est eorum multitudo, qui per additionem duorum quadratorum produci nequeunt, in eorum naturam et proprietates, qui sunt summae duorum quadratorum, hic inquiram. Quarum proprietatum etiamsi pleraeque iam sint cognitae et quasi per inductionem erutae, tamen firmis demonstrationibus maximam partem destituuntur; quarum veritati cum haud contemnenda pars Analyseos DIOPHANTEAE innitatur, in hac dissertatione plurium huiusmodi propositionum, quae adhuc sine demonstrationibus sunt admissae, demonstrationes adornabo, simul vero etiam eas commemorabo, quas mihi quidem etiamnunc demonstrare non licuit, etiamsi de earum veritate nullo modo dubitare queamus.

2. Primum igitur, cum numeri quadrati sint

0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196 etc.,

istos numeros, qui ex combinatione binorum quadratorum oriuntur, inspexisse iuvabit, quos propterea usque ad 200 hic apponam:

0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37, 40, 41, 45, 49, 50, 52, 53, 58, 61, 64, 65, 68, 72, 73, 74, 80, 81, 82, 85, 89, 90, 97, 98, 100, 101, 104, 106, 109, 113, 116, 117, 121, 122, 125, 128, 130, 136, 137, 144, 145, 146, 148, 149, 153, 157, 160, 162, 164, 169, 170, 173, 178, 180, 181, 185, 193, 194, 196, 197, 200.

1) Vide Commentationes 158 et 191 huius voluminis. F. R.

Hi nempe omnes sunt numeri usque ad 200, qui ex additione duorum quadratorum proveniunt, hosque numeros cum omnibus in infinitum sequentibus vocabo summas duorum quadratorum, quos idcirco in hac formula generali $xx+yy$ comprehendi manifestum est, dum pro x et y successive omnes numeri integri 0, 1, 2, 3, 4, 5, 6 etc. substituuntur. Qui igitur numeri in his non reperiuntur, ii non sunt summae duorum quadratorum; qui ergo sunt usque ad 200:

3, 6, 7, 11, 12, 14, 15, 19, 21, 22, 23, 24, 27, 28, 30, 31, 33, 35, 38, 39, 42, 43, 44, 46, 47, 48, 51, 54, 55, 56, 57, 59, 60, 62, 63, 66, 67, 69, 70, 71, 75, 76, 77, 78, 79, 83, 84, 86, 87, 88, 91, 92, 93, 94, 95, 96, 99, 102, 103, 105, 107, 108, 110, 111, 112, 114, 115, 118, 119, 120, 123, 124, 126, 127, 129, 131, 132, 133, 134, 135, 138, 139, 140, 141, 142, 143, 147, 150, 151, 152, 154, 155, 156, 158, 159, 161, 163, 165, 166, 167, 168, 171, 172, 174, 175, 176, 177, 179, 182, 183, 184, 186, 187, 188, 189, 190, 191, 192, 195, 198, 199.

Unde patet saltem usque ad 200 multitudinem numerorum, qui non sunt summae duorum quadratorum, maiorem esse quam eorum, qui sunt summae duorum quadratorum. Ceterum inspicienti statim patebit neutram istorum numerorum seriem certa et assignabili lege contineri atque ob hoc ipsum difficilius erit utriusque indolem investigare.

3. Cum omnis numerus quadratus sit vel par hocque casu per 4 divisibilis et in hac forma $4a$ contentus, vel impar hocque casu in hac forma $8b+1$ contineatur, omnis numerus ex duobus quadratis compositus erit:

Vel primo summa duorum quadratorum parium et ad hanc formam $4a+4b$ pertinebit eritque ergo per 4 divisibilis;

vel secundo summa duorum quadratorum alterius paris alterius imparis et propterea in huiusmodi forma $4a+8b+1$ seu in hac $4a+1$ continebitur; unitate ergo excedet multiplum quaternarii;

vel tertio summa duorum quadratorum imparium eritque idcirco huius formae $8a+1+8b+1$ seu in hac $8a+2$ continebitur; erit scilicet numerus impariter par et binario excedet multiplum octonarii.

Quia ergo omnes numeri impares vel unitate excedunt multiplum quaternarii seu huius sunt formae $4n+1$, vel unitate deficiunt a multiplo quaternarii seu huius sunt formae $4n-1$, patet nullos numeros impares huius

posterioris formae $4n-1$ esse summas duorum quadratorum; seu ex serie numerorum, qui sunt summae duorum quadratorum, excluduntur omnes numeri in hac forma contenti $4n-1$.

Deinde quia omnes numeri impariter pares vel binario superant multiplum octonarii, ut sint $8n+2$, vel binario deficiunt a multiplo octonarii, ut sint $8n-2$, patet nullos numeros huius posterioris formae esse summas duorum quadratorum; sicque ex serie numerorum, qui sunt summae duorum quadratorum, excluduntur numeri huius formae $8n-2$.

Interim tamen probe observandum est neque omnes numeros in hac forma $4n+1$ neque in hac $8n+2$ contentos esse summas duorum quadratorum. Illius enim formae excluduntur numeri 21, 33, 57, 69, 77, 93, 105, 129 etc., huius vero isti 42, 66, 114, 138, 154 etc., quorum ratio deinceps investigabitur.

4. Interim tamen numeri, qui sunt summae duorum quadratorum, ita nexu quodam inter se coniunguntur, ut ex uno huius indolis numero infiniti alii eiusdem naturae assignari queant. Quod quo facilius perspiciatur, sequentia lemmata, quae quidem vulgo satis sunt nota, adiungam.

I. *Si numerus p sit summa duorum quadratorum, erunt quoque numeri $4p$, $9p$, $16p$ et generatim nnp summae duorum quadratorum.*

Cum enim sit $p=aa+bb$, erit

$$4p=4aa+4bb,\quad 9p=9aa+9bb,\quad 16p=16aa+16bb \quad \text{et} \quad nnp=nnaa+nnbb,$$

quae formulae sunt pariter summae duorum quadratorum.

II. *Si numerus p sit summa duorum quadratorum, erit quoque $2p$ et generatim $2nnp$ summa duorum quadratorum.*

Sit enim $p=aa+bb$; erit $2p=2aa+2bb$. Sed est

$$2aa+2bb=(a+b)^2+(a-b)^2,$$

unde erit

$$2p=(a+b)^2+(a-b)^2$$

ac propterea summa duorum quadratorum. Hinc vero porro erit

$$2nnp=nn(a+b)^2+nn(a-b)^2.$$

III. *Si numerus par $2p$ fuerit summa duorum quadratorum, erit etiam eius semissis p summa duorum quadratorum.*

Sit enim $2p = aa + bb$; erit numerorum a et b uterque vel par vel impar, unde utroque casu erit tam $\frac{a+b}{2}$ quam $\frac{a-b}{2}$ numerus integer. Est vero

$$aa + bb = 2\left(\frac{a+b}{2}\right)^2 + 2\left(\frac{a-b}{2}\right)^2,$$

quo valore substituto fit

$$p = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2.$$

Hinc ergo omnes numeri pares, qui sunt summae duorum quadratorum, per continuam bisectionem tandem revocantur ad numeros impares eiusdem indolis. Quare vicissim si soli numeri impares, qui sunt summae duorum quadratorum, cognoscantur, ex iis omnes quoque pares per continuam duplicationem derivabuntur.

5. Deinde notatu dignum est sequens theorema, quo natura numerorum, qui sunt summae duorum quadratorum, non mediocriter illustratur.

THEOREMA

Si p et q sint duo numeri, quorum uterque est summa duorum quadratorum, erit etiam eorum productum pq summa duorum quadratorum.

DEMONSTRATIO

Sit $p = aa + bb$ et $q = cc + dd$; erit

$$pq = (aa + bb)(cc + dd) = aacc + aadd + bbcc + bbdd,$$

quae expressio hoc modo repraesentari potest, ut sit

$$pq = aacc + 2abcd + bbdd + aadd - 2abcd + bbcc$$

ideoque

$$pq = (ac + bd)^2 + (ad - bc)^2;$$

unde productum pq erit summa duorum quadratorum. Q. E. D.

Ex hac propositione sequitur, quomodocunque plures numeri, qui singuli sint summae duorum quadratorum, invicem multiplicentur, producta semper esse summas duorum quadratorum. Atque ex forma generali tradita patet productum ex duobus huiusmodi numeris duplici modo in duo quadrata resolvi posse. Si enim sit $p = aa + bb$ et $q = cc + dd$, erit tam

$$pq = (ac + bd)^2 + (ad - bc)^2$$

quam

$$pq = (ac - bd)^2 + (ad + bc)^2,$$

quae formulae erunt diversae, nisi sit vel $a = b$ vel $c = d$. Sic cum sit $5 = 1 + 4$ et $13 = 4 + 9$, productum $5 \cdot 13 = 65$ duplici modo erit summa duorum quadratorum,[1]) scilicet erit

$$65 = (1 \cdot 3 + 2 \cdot 2)^2 + (2 \cdot 3 - 1 \cdot 2)^2 = 49 + 16$$

et

$$65 = (2 \cdot 2 - 1 \cdot 3)^2 + (2 \cdot 3 + 1 \cdot 2)^2 = 1 + 64.$$

Atque si productum habeatur ex pluribus numeris, qui singuli sint summae duorum quadratorum, id pluribus modis in duo quadrata resolvi poterit. Uti si proponatur numerus $1105 = 5 \cdot 13 \cdot 17$, eius resolutiones in duo quadrata erunt hae

$$1105 = 33^2 + 4^2 = 32^2 + 9^2 = 31^2 + 12^2 = 24^2 + 23^2.$$

Quatuor scilicet hic resolutiones locum habent.

6. Quanquam autem ita evictum est, si factores p et q sint summae duorum quadratorum, etiam fore productum pq summam duorum quadratorum, tamen huius propositionis conversa hinc non sequitur, ut, si productum sit duorum quadratorum summa, etiam eius factores sint numeri eiusdem naturae; neque enim hanc conclusionem regulae logicae neque ipsa rei natura probarent. Nam numerus $45 = 36 + 9$ est summa duorum quadratorum, interim tamen horum factorum eius 3, 15 neuter est summa duorum quadratorum. Magis autem firma videatur haec conclusio: si productum pq et alteruter eius factor p fuerint duorum quadratorum summae, alterum quoque factorem q fore summam duorum quadratorum. Tametsi autem haec conclusio forte sit vera, regulis tamen ratiocinandi non confirmatur; neque enim, cum demon-

1) Hoc exemplum invenitur iam in quaestione XIX libri III Diophanti *Arithmeticorum* (ed. Tannery; quae quaestio est quaestio XXII editionis Bacheti); vide notam p. 404 huius voluminis. F. R.

stratum sit, si producti pq bini factores p et q sint duorum quadratorum summae, ipsum pq fore summam duorum quadratorum, hinc legitima consequentia inferri potest: si et productum pq et alter factor p sint summae duorum quadratorum, etiam alterum factorem q fore summam duorum quadratorum. Huiusmodi enim consequentiam non esse legitimam vel hoc exemplum evidenter evincet: Certum est, si bini factores p et q sint numeri pares, etiam productum pq fore numerum parem; si quis autem hinc concludere velit, si productum pq et alter factor p sint numeri pares, etiam alterum factorem q fore parem, is vehementer falleretur.

7. Quare si verum sit, ut, cum productum pq et alter eius factor p fuerint summae duorum quadratorum, alter quoque factor q sit summa duorum quadratorum, haec propositio non ex ante demonstrata potest inferri, sed peculiari demonstratione muniri debet. Haec autem demonstratio non tam plana est quam praecedens et non nisi per plures ambages concinnari potest; ac demonstratio quidem, quam inveni, ita comparata videtur, ut non mediocrem vim ratiocinii requirat. Hanc ob rem propositiones, ex quibus tandem non solum haec veritas conficitur, sed etiam aliae insignes proprietates huiusmodi numerorum, qui sunt summae duorum quadratorum, cognoscuntur, cum suis demonstrationibus hic ordine proponam operamque dabo, ut nihil quicquam in rigore demonstrandi desiderari queat. Iis autem, quae hactenus de his numeris praemisi, uti sunt trivia et in vulgus nota, ita instar lemmatum in sequentibus demonstrationibus utar.

PROPOSITIO 1

8. *Si productum pq sit summa duorum quadratorum et alter factor p sit numerus primus pariterque duorum quadratorum summa, erit quoque alter factor q summa duorum quadratorum.*

DEMONSTRATIO

Sit $pq = aa + bb$ et $p = cc + dd$; quia p est numerus primus, erunt c et d numeri inter se primi. Erit itaque

$$q = \frac{aa + bb}{cc + dd}$$

et propterea ob q numerum integrum numerator $aa+bb$ per denominatorem $cc+dd$ erit divisibilis. Hinc quoque per $cc+dd$ divisibilis erit numerus

$$cc(aa+bb) = aacc + bbcc;$$

at cum etiam hic numerus

$$aa(cc+dd) = aacc + aadd$$

per $cc+dd$ sit divisibilis, horum numerorum differentia

$$aacc + bbcc - aacc - aadd \quad \text{seu} \quad bbcc - aadd$$

per $cc+dd$ divisibilis sit necesse est. Cum autem sit $cc+dd$ numerus primus et $bbcc-aadd$ factores habeat $bc+ad$ et $bc-ad$, alteruter horum factorum, nempe $bc\pm ad$, per $cc+dd$ erit divisibilis. Sit itaque

$$bc \pm ad = mcc + mdd;$$

quicunque autem numeri sint a et b, ii ita exprimi possunt, ut sit $b=mc+x$ et $a=\pm md+y$ existentibus x et y numeris integris sive affirmativis sive negativis. His vero valoribus pro b et a substitutis aequatio

$$bc \pm ad = mcc + mdd$$

induet hanc formam

$$mcc + cx + mdd \pm dy = mcc + mdd$$

seu

$$cx \pm dy = 0.$$

Hinc erit $\frac{x}{y} = \mp\frac{d}{c}$, et quia d et c sunt numeri primi inter se, necesse est, ut sit $x=nd$ et $y=\mp nc$, unde habebitur

$$a = \pm md \mp nc \quad \text{et} \quad b = mc + nd;$$

huiusmodi scilicet valores habere debebunt numeri a et b, ut numerus $pq=aa+bb$ sit divisibilis per numerum primum $p=cc+dd$. Verum istis valoribus pro a et b substitutis fiet

$$pq = mmdd - 2mncd + nncc + mmcc + 2mncd + nndd$$

seu

$$pq = (mm+nn)(cc+dd).$$

Iam ob $p = cc + dd$ erit

$$q = mm + nn;$$

ideoque si productum pq fuerit summa duorum quadratorum $aa + bb$ et alter factor p sit numerus primus pariterque duorum quadratorum summa $cc + dd$, necessario sequitur etiam alterum factorem q fore summam duorum quadratorum. Q. E. D.

COROLLARIUM 1

9. Si ergo summa duorum quadratorum divisibilis sit per numerum primum, qui ipse sit summa duorum quadratorum, etiam quotus ex divisione resultans erit summa duorum quadratorum. Ita si summa duorum quadratorum fuerit divisibilis per quempiam ex his numeris primis 2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97 etc., quotus semper erit summa duorum quadratorum.

COROLLARIUM 2

10. Si ergo litterae α, β, γ, δ etc. denotent huiusmodi numeros primos, qui sunt summae duorum quadratorum, hinc patet, si productum αq sit summa duorum quadratorum, fore etiam factorem q summam duorum quadratorum.

COROLLARIUM 3

11. Hinc autem porro facile colligitur, si productum $\alpha\beta q$ fuerit summa duorum quadratorum, fore etiam factorem q summam duorum quadratorum. Cum enim sit $\alpha\beta q$ summa duorum quadratorum, per corollarium praecedens erit quoque βq summa duorum quadratorum; et ob eandem rationem erit quoque q summa duorum quadratorum.

COROLLARIUM 4

12. Simili modo evidens est, si productum $\alpha\beta\gamma\delta\varepsilon q$ fuerit summa duorum quadratorum, tum quoque factorem q esse summam duorum quadratorum; hinc si productum pq sit summa duorum quadratorum eiusque factor p productum ex quotcunque numeris primis, quorum singuli sint summae duorum quadratorum, fore etiam alterum factorem q summam duorum quadratorum.

SCHOLION

13. Regulae logicae non permittunt, ut haec propositio ita convertatur, ut, quoties alter factor q sit summa duorum quadratorum, etiam alter factor p pronunciari possit vel summa duorum quadratorum, si est primus, vel productum ex numeris primis, qui singuli sint summae duorum quadratorum. De hoc ipso enim nondum constat, utrum productum ex aliquot numeris primis, qui ipsi non sint summae duorum quadratorum, nequeat esse summa duorum quadratorum; quin potius contrario iam habemus casum, quo productum $45 = 3 \cdot 3 \cdot 5$ est summa duorum quadratorum, cum tamen eius factores 3 et 3 non sint huius indolis. Verum propositio corollarii ultimi ita converti potest, ut a negatione consequentis recte ad negationem antecedentis concludatur, quam conversionem utpote maximi momenti in hac propositione complectar.

PROPOSITIO 2

14. *Si productum pq sit summa duorum quadratorum, eius factor autem q non sit summa duorum quadratorum, tum alter factor p, si sit numerus primus, non erit summa duorum quadratorum, sin autem non sit primus, saltem factorem certe habebit primum, qui non sit summa duorum quadratorum.*

DEMONSTRATIO

Cum alter factor p sit vel numerus primus vel compositus, utrumque casum seorsim perpendere convenit. Sit primo p numerus primus; cum igitur, si esset summa duorum quadratorum, quoque alter factor q foret summa duorum quadratorum, quod cum hypothesi adversetur, sequitur factorem p non esse summam duorum quadratorum. Sit secundo p numerus compositus et ex praecedentibus liquet, si omnes eius factores primi essent summae duorum quadratorum, etiam alterum factorem q eiusdem fore indolis. Quare cum per hypothesin q non sit summa duorum quadratorum, sequitur non omnes factores ipsius p esse summas duorum quadratorum. Q. E. D.

COROLLARIUM 1

15. Si igitur productum pq sit summa duorum quadratorum, eius tamen alter factor q in duo quadrata sit irresolubilis, alter factor p vel ipse non

erit summa duorum quadratorum vel saltem factorem habebit primum in duo quadrata irresolubilem. Uti si sit $pq = 45$ et $q = 3$, erit $p = 15$ et factorem habet 3, qui non est summa duorum quadratorum.

COROLLARIUM 2

16. Hinc autem nondum concludere licet alterum factorem p plane non esse summam duorum quadratorum; quamvis enim hoc certum sit casu, quo p est numerus primus, tamen id nondum constat casu, quo p est numerus compositus, quia p habere posset factorem in duo quadrata irresolubilem, etiamsi ipse numerus p esset summa duorum quadratorum.

COROLLARIUM 3

17. Hoc autem colligere licet: Si p esset summa duorum quadratorum, tum non solum unum, sed ad minimum duos habere debere factores primos in duo quadrata irresolubiles. Sit enim $p = \alpha\beta\gamma\delta$ et δ factor ille in duo quadrata irresolubilis; perspicuum est, si p esset summa duorum quadratorum, deleto factore δ insuper factorem residuum $\alpha\beta\gamma$ factorem in duo quadrata irresolubilem habere debere.

SCHOLION

18. Cum de divisoribus numerorum, qui sunt summae duorum quadratorum, quaestio instituitur, circa quadratorum summam $aa + bb$ casus hi probe sunt distinguendi, utrum haec quadrata aa et bb seu eorum radices a et b sint numeri primi inter se necne. Si enim a et b non sint numeri primi inter se, sed habeant communem divisorem n, ut sit $a = nc$ et $b = nd$, summa quadratorum erit $nncc + nndd = nn(cc + dd)$ ac propterea divisorem habebit n, hoc est, numerum quemcunque. Sin autem radices a et b fuerint numeri primi inter se, tum summa quadratorum $aa + bb$ plures numeros pro divisoribus non admittet; evidens enim est huiusmodi summam duorum quadratorum $aa + bb$ nunquam per 3 esse divisibilem. Nam quia per hypothesin utrumque quadratum seorsim non est per 3 divisibile, cum alioquin non forent prima inter se, si summa $aa + bb$ esset per 3 divisibilis, neutrum foret per 3 divisibile. Utriusque ergo radices futurae essent vel huius formae $3m + 1$ vel huius $3m - 1$; sed summa huiusmodi duorum quadratorum per 3 divisa semper residuum 2 relinquit ideoque per 3 nunquam est divisibilis. Eodem

modo intelligitur summam duorum quadratorum inter se primorum $aa+bb$ nunquam esse per 7 vel 11 vel 19 etc. divisibilem. Quinam autem sint in genere hi numeri, qui nunquam summae duorum quadratorum inter se primorum divisores existere queant, hoc modo non facile definitur. Demonstrari igitur convenit propositionem alias[1]) quidem satis notam summam duorum quadratorum inter se primorum alios divisores primos non admittere, nisi qui ipsi sint summae duorum quadratorum. Praemitti autem debet sequens propositio.

PROPOSITIO 3

19. *Si summa duorum quadratorum inter se primorum $aa+bb$ divisibilis sit per numerum p, semper exhiberi poterit summa duorum aliorum quadratorum $cc+dd$ divisibilis per eundem numerum p, ita ut ista summa $cc+dd$ non sit maior quam $\frac{1}{2}pp$.*

DEMONSTRATIO

Sit summa duorum quadratorum inter se primorum $aa+bb$ divisibilis per numerum p et a et b numeri quantumvis magni. Quia ergo neque a neque b seorsim per p divisibilis est, numeri a et b ita exprimi poterunt, ut sit $a=mp\pm c$ et $b=np\pm d$, ubi numeros m et n ita determinare licet, ut c et d non excedant semissem ipsius p. Erit ergo

$$aa+bb=mmpp\pm 2mcp+cc+nnpp\pm 2ndp+dd;$$

quae formula cum et tota divisibilis sit per p (per hypothesin) et eius pars $mmpp\pm 2mcp+nnpp\pm 2ndp$ per se divisorem habeat p, necesse est, ut altera pars $cc+dd$, quae est summa duorum quadratorum, itidem per p sit divisibilis. At cum radices c et d non excedant semissem ipsius p, summa quadratorum $cc+dd$ non excedet quadratum $\frac{1}{4}pp$ bis sumtum; ideoque summa duorum quadratorum $cc+dd$ exhiberi potest non maior quam $\frac{1}{2}pp$, quae tamen sit per p divisibilis. Q. E. D.

1) Vide § 20 Commentationis 134 huius voluminis, imprimis notam p. 70. F. R.

COROLLARIUM 1

20. Si igitur non detur summa duorum quadratorum inter se primorum divisibilis per numerum p, quae non excedat $\frac{1}{2}pp$, nullae omnino dantur summae duorum quadratorum inter se primorum, quae per hunc numerum p essent divisibiles.

COROLLARIUM 2

21. Sic cum nulla detur summa duorum quadratorum inter se primorum infra $\frac{1}{2}\cdot 3^2$ seu infra $4\frac{1}{2}$, quae sit per 3 divisibilis, hinc luculenter sequitur nullam omnino summam duorum quadratorum inter se primorum per 3 esse divisibilem. Similique modo pro numero 7, cum non detur summa duorum quadratorum infra $\frac{1}{2}\cdot 7^2 = 24\frac{1}{2}$ per 7 divisibilis, sequitur ne in maximis quidem numeris dari summas duorum quadratorum inter se primorum per 7 divisibiles.

PROPOSITIO 4

22. *Summa duorum quadratorum inter se primorum dividi nequit per ullum numerum, qui ipse non sit summa duorum quadratorum.*

DEMONSTRATIO

Ad hoc demonstrandum ponamus summam duorum quadratorum inter se primorum $aa + bb$ divisibilem esse per numerum p, qui non sit summa duorum quadratorum. Exhiberi ergo posset alia summa duorum quadratorum inter se primorum $cc + dd$ non maior quam $\frac{1}{2}pp$, quae esset divisibilis per p. Sit igitur $cc + dd = pq$, et cum p non sit summa duorum quadratorum, vel ipse numerus q non erit eiusmodi summa vel saltem factorem habebit r, qui non erit summa duorum quadratorum. Quia vero $pq < \frac{1}{2}pp$, erit $q < \frac{1}{2}p$ et multo magis $r < \frac{1}{2}p$. Quare cum $cc + dd$ quoque divisibilis sit per $r < \frac{1}{2}p$, per propositionem praecedentem summa duorum quadratorum $ee + ff$ per eundem numerum r divisibilis exhiberi posset, quae non excederet $\frac{1}{2}rr$ neque multo magis $\frac{1}{8}pp$. Et cum r non sit summa duorum quadratorum, simili modo procedendo continuo ad minores summas duorum quadratorum deveniretur, quae per numerum non-summam duorum quadratorum essent

divisibiles. Quocirca, cum in minimis numeris nulla detur summa duorum quadratorum inter se primorum, quae esset divisibilis per numerum, qui non sit summa duorum quadratorum, ne in maximis quidem numeris eiusmodi erunt summae duorum quadratorum, quae divisibiles sint per numeros, qui ipsi non essent summae duorum quadratorum. Q. E. D.

COROLLARIUM 1

23. Si ergo summa duorum quadratorum inter se primorum non fuerit numerus primus, omnes eius factores primi quoque erunt summae duorum quadratorum. Quemadmodum igitur productum ex quotcunque numeris primis, qui ipsi sunt summae duorum quadratorum, pariter est summa duorum quadratorum, ita nunc huius propositionis conversa est demonstrata, ut summa duorum quadratorum (inter se primorum) per multiplicationem oriri nequeat, nisi ex numeris, qui ipsi sint summae duorum quadratorum.

COROLLARIUM 2

24. Omnes ergo numeri, qui sunt summae duorum quadratorum inter se primorum, vel ipsi in hac serie numerorum primorum continentur

$$2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113 \text{ etc.}$$

vel ex duobus pluribusve numeris huius seriei per multiplicationem componuntur. Omnes autem hi numeri primi praeter 2 unitate excedunt multiplum quaternarii seu in hac forma $4n + 1$ continentur.

COROLLARIUM 3

25. Si igitur summa duorum quadratorum $aa + bb$ divisibilis sit per numerum, qui non fuerit summa duorum quadratorum, hinc intelligetur quadrata illa aa et bb non esse inter se prima neque adeo eorum radices a et b.

COROLLARIUM 4

26. Cum autem, si $a = nc$ et $b = nd$, summa duorum quadratorum $aa + bb = nn(cc + dd)$ per quemvis numerum n, qui non est summa duorum quadratorum, dividi possit, quoniam non solum per n, sed etiam per nn est divisibilis, evidens est, si summa duorum quadratorum divisibilis sit per

quempiam numerum, qui non est summa duorum quadratorum, tum eam quoque per quadratum huius numeri fore divisibilem. Sic cum $45 = 36 + 9$ sit divisibilis per 3, simul quoque divisibilis est per 9.

COROLLARIUM 5

27. Cum nullus numerorum in hac forma $4n - 1$ contentorum sit summa duorum quadratorum[1]), manifestum quoque est nullam summam duorum quadratorum inter se primorum dividi posse per ullum numerum primum in forma $4n - 1$ contentum, qui numeri primi sunt

3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107 etc.

SCHOLION

28. Cum omnes numeri primi, qui sunt summae duorum quadratorum, excepto binario hanc seriem constituant

5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149 etc.,

qui non solum in hac forma $4n + 1$ continentur, sed etiam, quantumvis ea longe continuetur, deprehendemus in ea omnes omnino numeros primos huius formae $4n + 1$ occurrere, unde per inductionem satis probabiliter concludere licet nullum dari numerum primum formae $4n + 1$, qui non simul sit summa duorum quadratorum. Interim tamen cum inductio quantumvis ampla vicem demonstrationis sustinere nequeat, hanc veritatem, quod omnis numerus primus formae $4n + 1$ simul sit summa duorum quadratorum, etiamsi nemo agnoscere dubitet, tamen adhuc demonstratis matheseos veritatibus annumerare non licet. FERMATIUS[2]) quidem professus est se eius demonstrationem

1) Vide § 20 Commentationis 134 huius voluminis, imprimis notam p. 70. F. R.

2) Hoc celebre theorema FERMATIUS a. 1640 cum amico MERSENNE sine demonstratione communicavit, *Oeuvres de FERMAT*, t. II, p. 212. Vide etiam FERMATII epistolam a. 1658 ad KENELMUM DIGBY datam (epist. XLVI *Commercii epistolici* a WALLISIO a. 1658 primo editi), I. WALLIS, *Opera*, t. II, Oxoniae 1693, p. 857; *Oeuvres de FERMAT*, t. II, p. 402. Cf. praeterea FERMATII epistolas ad FRENICLE (1641), PASCAL (1654), CARCAVI (1659) scriptas, *Oeuvres de FERMAT*, t. II, p. 221, 310, 431. Vide porro FERMATII observationem ad BACHETI commentarium in quaestionem XIX libri III DIOPHANTI *Arithmeticorum* (ed. TANNERY; quae quaestio est quaestio XXII editionis BACHETI; cf. notam p. 404 et notam 2 p. 51 huius voluminis); *Oeuvres de FERMAT*, t. I, p. 293. F. R.

invenisse; quia autem eam nusquam publicavit, asserto quidem huius profundissimi Viri merito fidem adhibemus istamque numerorum proprietatem credimus; haecque cognitio nostra mera fide sine scientia nititur. Quanquam autem ego multum in demonstratione eruenda frustra laboravi, tamen aliud argumentum pro hac veritate astruenda repperi, quod, etiamsi non summum rigorem sustineat, tamen cum inductione coniunctum demonstrationi pene rigorosae aequivalere videtur.

PROPOSITIO 5

28[a][1]. *Omnis numerus primus, qui unitate excedit multiplum quaternarii, est summa duorum quadratorum.*

TENTAMEN DEMONSTRATIONIS

Numeri primi, de quibus hic sermo est, in hac forma $4n+1$ continentur. Quodsi ergo numerus $4n+1$ fuerit primus, demonstravi[2] per eum semper divisibilem esse hanc formam $a^{4n}-b^{4n}$, quicunque numeri pro a et b substituantur, dummodo neuter seorsim fuerit per $4n+1$ divisibilis. Cum autem sit $a^{4n}-b^{4n}=(a^{2n}-b^{2n})(a^{2n}+b^{2n})$, necesse est, ut alteruter factor, nempe vel $a^{2n}-b^{2n}$ vel $a^{2n}+b^{2n}$, sit divisibilis per numerum primum $4n+1$. Prout autem pro a et b alii atque alii numeri assumuntur, aliis casibus formula $a^{2n}-b^{2n}$, aliis vero formula $a^{2n}+b^{2n}$ erit per $4n+1$ divisibilis, unde assumere licet, etsi quidem hoc nondum firma demonstratione[3] evincere valeo, semper eiusmodi numeros pro a et b assignari posse, ut formula $a^{2n}-b^{2n}$ non sit per $4n+1$ divisibilis; iis ergo casibus altera formula $a^{2n}+b^{2n}$ necessario per $4n+1$ erit divisibilis. Sit $a^n=p$ et $b^n=q$ habebiturque summa duorum quadratorum $pp+qq$ per $4n+1$ divisibilis, ita ut neutrum quadratum pp vel qq seorsim habeat divisorem $4n+1$. Ideoque etiamsi fortasse pp et qq communem habeant divisorem mm, ut sit $pp+qq=mm(rr+ss)$, quia factor communis mm divisorem non habet $4n+1$, necesse est, ut summa duorum quadratorum inter se primorum

1) In editione principe falso numerus 28 iteratur. F. R.

2) Vide Commentationem 134 huius voluminis, imprimis theorema 4. F. R.

3) Firmam demonstrationem EULERUS paulo post dedit in Commentatione 241 huius voluminis. F. R.

$rr + ss$ habeat divisorem $4n + 1$. Consequenter, cum huiusmodi summa duorum quadratorum alios non admittat divisores, nisi qui ipsi sint summae duorum quadratorum, necesse est, ut numerus primus $4n + 1$ sit summa duorum quadratorum.

COROLLARIUM 1

29. Demonstratio haec igitur esset perfecta, si modo demonstrari posset semper eiusmodi existere valores pro a et b substituendos, quibus formula $a^{2n} - b^{2n}$ non fiat divisibilis per numerum primum $4n + 1$; iisdem enim casibus formula $a^{2n} + b^{2n}$ necessario est divisibilis per $4n + 1$.

COROLLARIUM 2

30. Quodsi quis autem hanc rem per calculum tentet, non modo semper plures casus, immo infinitos, formulae $a^{2n} - b^{2n}$ reperiet, quibus ea per numerum primum $4n + 1$ non est divisibilis, sed etiam pro b unitatem ponere licet, ita ut etiam haec formula simplicior $a^{2n} - 1$ saepenumero per $4n + 1$ non sit divisibilis.

SCHOLION

31. Casus seu valores ipsius a, quibus formula $a^{2n} - 1$ certe fit divisibilis per numerum primum $4n + 1$, facile assignari possunt. Primo enim si sit $a = pp$, formula $a^{2n} - 1 = p^{4n} - 1$ semper est divisibilis per $4n + 1$, dummodo p non sit $= 4n + 1$ vel eius multiplo. Deinde si $a = pp \pm (4n + 1)q$, formula $a^{2n} - 1$ quoque divisorem habet $4n + 1$; resolvitur enim

$$a^{2n} = (pp \pm (4n + 1)q)^{2n}$$

in seriem terminorum, quorum primus est p^{4n}, sequentes vero omnes sponte sunt per $4n + 1$ divisibiles. Unde patet valores idoneos pro a esse omnia residua, quae restant, si numeri quadrati p^2 per $4n + 1$ dividantur.[1]) Haec autem residua, sive pro a ponatur r sive $4n + 1 + r$ sive $(4n + 1)q + r$, prodeunt eadem, unde omnia possibilia residua obtinentur, si pro p successive statuantur numeri 1, 2, 3, 4, 5, ... usque ad $4n$; at valor $4n$ pro p positus idem dat residuum, quod valor 1, similique modo valores 2 et $4n - 1$, item 3 et $4n - 2$, item 4 et $4n - 3$ etc. eadem dant residua. Unde cum bina

1) Vide Commentationes 134 (imprimis theorema 11) et 242 huius voluminis. F. R.

semper residua, quae ex numeris 1, 2, 3, ... usque ad $4n$ pro radicibus quadratorum sumtis proveniunt, sint aequalia, numerus diversorum residuorum resultantium tantum erit $2n$ ideoque totidem dabuntur numeri ipso $4n+1$ minores, qui non esse possunt residua ex divisione numerorum quadratorum per $4n+1$ emergentia; hique numeri pro a substituti semper formulam $a^{2n}-1$ reddent non divisibilem per $4n+1$. Hoc quidem pariter demonstrari nequit; verumtamen, quia periculum faciendo, quotcunque etiam numeri hoc modo explorentur, ne unicus quidem casus occurret, quo haec regula fallat, eius veritatem agnoscere oportet.

Quo haec clarius perspiciantur, exempla aliquot subiungam. Sit primo $4n+1=5$ et casus, quibus formula a^2-1 per 5 erit divisibilis, habebuntur, si pro a residua ex divisione quadratorum per 5 oriunda ponantur, quae residua sunt 1, 4. At si pro a ponatur vel 2 vel 3, formula a^2-1 non erit per 5 divisibilis; his ergo casibus formula a^2+1 divisorem habebit 5. Deinde si sit $4n+1=13$ seu $n=3$, residua, quae ex divisione numerorum quadratorum per 13 restant, sunt 1, 4, 9, 3, 12, 10; unde si quis numerorum reliquorum 2, 5, 6, 7, 8, 11 pro a substituatur, non formula a^6-1, sed a^6+1 per 13 erit divisibilis. Porro si $4n+1=17$ seu $n=4$, quia residua quadratorum per 17 divisorum sunt 1, 4, 9, 16, 8, 2, 15, 13, si pro a statuatur quispiam ex reliquis numeris 3, 5, 6, 7, 10, 11, 12, 14, non formula a^8-1, sed haec a^8+1 erit per 17 divisibilis. Cum igitur haec lex perpetuo observetur, haec inductio vim demonstrationis fere induere censenda erit; hincque propositio tantopere confirmata videtur, ut eius veritatem non amplius in dubium vocare liceat. Interim tamen operae pretium esset eo maius, si quis rigorosam huius propositionis demonstrationem exhibere posset, quo magis de eius veritate sumus certi; nullum enim est dubium, quin eiusmodi demonstratio tamdiu frustra quaesita ad plurimas alias insignes numerorum proprietates sit manuductura. Quanquam autem huius propositionis veritas extra dubium est posita, tamen eas consequentias, quae ipsi innituntur, diligenter notabo ab aliisque, quae rigidis demonstrationibus muniuntur, distinguam; ex hac autem propositione nondum demonstrata sequuntur haec corollaria, quae hoc nomine notata velim.

COROLLARIUM 3

32. Si igitur numerus formae $4n+1$ in duo quadrata nullo modo resolvi nequeat, hoc certum erit signum eum numerum non esse primum

si enim iste numerus $4n+1$ esset primus, certe in duo quadrata resolvi posset. Sic cum numeri 21, 33, 57, 69, 77, 93 etc., qui in forma $4n+1$ continentur, non sint summae duorum quadratorum, ex hoc ipso patet eos non esse primos.

COROLLARIUM 4

33. In serie ergo numerorum, qui sunt summae duorum quadratorum, omnes primo continentur numeri primi huius formae $4n+1$, deinde omnia producta ex duobus pluribusve huiusmodi numeris primis, tum producta ex singulis hisce numeris in binarium et quosvis numeros quadratos.

COROLLARIUM 5

34. Omnes numeri n, ex quibus formula $4n+1$ evadit numerus primus, sunt summae duorum numerorum trigonalium. Cum enim $4n+1$ sit summa duorum quadratorum, erit eius duplum $8n+2$ summa duorum quadratorum imparium [§ 4]. Sit ergo

$$8n+2=(2x+1)^2+(2y+1)^2;$$

fiet

$$n=\frac{xx+x}{2}+\frac{yy+y}{2}.$$

Quare si n non sit summa duorum numerorum trigonalium, certe numerus $4n+1$ non erit primus.

PROPOSITIO 6

35. *Si numerus formae $4n+1$ unico modo in duo quadrata inter se prima resolvi queat, tum certe est numerus primus.*

DEMONSTRATIO

Quoniam enim hic numerus est summa duorum quadratorum inter se primorum, si non sit primus, singuli eius factores erunt summae duorum quadratorum [§ 22]. Quare si hic numerus non esset primus, in huiusmodi saltem duos factores resolvi posset, ut esset $4n+1=(aa+bb)(cc+dd)$; hoc autem casu duplex resolutio in duo quadrata locum habet [§ 5], scilicet

$$\text{I.} \quad 4n + 1 = (ac + bd)^2 + (ad - bc)^2,$$

$$\text{II.} \quad 4n + 1 = (ad + bc)^2 + (ac - bd)^2.$$

Haeque resolutiones semper sunt diversae, nisi sit vel $ac + bd = ad + bc$ vel $ac + bd = ac - bd$. Priori vero casu foret $ac + bd - ad - bc = 0$ seu $(a - b)(c - d) = 0$ ideoque vel $a = b$ vel $c = d$; atque hinc vel $aa + bb$ vel $cc + dd$ numerus par, quorum neutrum esse potest divisor ipsius $4n + 1$ utpote numeri imparis. Posteriori vero casu esset vel $b = 0$ vel $d = 0$ ideoque $4n + 1$ vel $= aa(cc + dd)$ vel $= cc(aa + bb)$; unde haec duo quadrata non forent prima inter se contra hypothesin. Quibus casibus notatis sequitur numerum compositum $4n + 1$, si in duo quadrata inter se prima fuerit resolubilis, eundem ad minimum duobus modis in duo quadrata esse resolubilem. Quocirca si tantum unico modo numerus $4n + 1$ sit summa duorum quadratorum, certe non erit compositus ac per consequens erit primus. Q. E. D.

COROLLARIUM 1

36. Si igitur proposito quopiam numero formae $4n + 1$ post institutum examen comperiatur eum unico modo in duo quadrata inter se prima resolvi posse, inde tuto colligemus eum numerum esse primum, etiamsi eius divisibilitatem per numeros primos more consueto non tentaverimus. Sic cum numerus 73 unico modo sit summa duorum quadratorum, nempe $64 + 9$, eum esse primum certo novimus.

COROLLARIUM 2

37. Si ergo methodus expedita haberetur, cuius ope facile inquirere liceret, an et quot modis propositus numerus in forma $4n + 1$ contentus in duo quadrata resolvi possit, exinde promte iudicare poterimus, utrum sit primus; si enim unico modo in duo quadrata sit resolubilis eaque quadrata fuerint prima inter se, is certe pro primo erit habendus.

COROLLARIUM 3

38. Manifestum autem est, si duo quadrata, in quae numerus quispiam resolvitur, non sint prima inter se, eum numerum non esse primum. Si enim numerus propositus inveniatur esse $= nnaa + nnbb$, tum divisores habebit n et nn; quod idem est intelligendum, si numerus propositus ipse sit quadratum seu $= aa + 0$; tum enim divisorem habebit a.

SCHOLION

39. Haec regula numeros primos explorandi tantum ad numeros impares formae $4n+1$ est adstricta; numeri enim pares quandoque unico modo in duo quadrata resolvi possunt, cum tamen non sint primi; ita 10 unico modo est summa duorum quadratorum, etsi non est primus, cuius rei ratio est, quod in producto $(aa+bb)(cc+dd)$, cui huiusmodi numeri aequantur, est vel $a=b$ vel $c=d$, quo casu duplex resolutio, quae generatim innui videtur, ad unam redit, uti in demonstratione est animadversum. Neque vero hac exceptione regula data infringitur, cum numerorum parium per se facile sit iudicium. Numeri autem impares alterius formae $4n-1$ hinc sponte excluduntur, quoniam ii plane non in duo quadrata sunt resolubiles. De cetero, si numerus $4n+1$ vel plane non resolubilis sit in duo quadrata vel pluribus modis haec resolutio succedat, pro priori casu iam notavimus eum numerum certe non esse primum, etsi hoc nititur propositione praecedente non satis rigide demonstrata. Pro casu vero posteriori in sequenti propositione iudicium afferetur.

PROPOSITIO 7

40. *Qui numerus duobus pluribusve diversis modis in duo quadrata resolvi potest, ille non est primus, sed ex duobus ad minimum factoribus compositus.*[1])

DEMONSTRATIO

Sit numerus propositus N, qui duplici modo in duo quadrata sit resolubilis, nempe

$$N=aa+bb=cc+dd.$$

Quoniam haec quadrata non sunt aequalia, alioquin enim numerus N per se non esset primus, sit $a>b$ et $c>d$, et quia resolutiones hae duae sunt diversae, neque erit $a=c$ neque $b=d$. Sit igitur $a>c$; erit $b<d$; unde ponatur $a=c+x$ et $d=b+y$. Quare ob $aa+bb=cc+dd$ fiet $2cx+xx=2by+yy$. Sit utraque forma $=xyz$, quia altera per x, altera per y est divisibilis; fiet

1) Hanc propositionem iam DIOPHANTUS cognosse videtur. Vide notam p. 301. F. R.

$$c = \frac{yz - x}{2}, \quad b = \frac{xz - y}{2}, \quad a = \frac{yz + x}{2}, \quad d = \frac{xz + y}{2}$$

hincque erit

$$N = aa + bb = \frac{xxzz + yy + yyzz + xx}{4} \quad \text{seu} \quad N = \frac{(yy + xx)(1 + zz)}{4}.$$

Nisi ergo $xx + yy$ per 4 sit divisibile, erit $xx + yy$ divisor ipsius N; sin autem $xx + yy$ sit per 4 divisibile vel numerus utcunque compositus, eius certe factor quidam erit divisor ipsius N. Cum igitur sit $x = a - c$ et $y = d - b$, numerus propositus $N = aa + bb = cc + dd$ divisorem habebit vel ipsum numerum $(a - c)^2 + (d - b)^2$ vel eius semissem quadrantemve, et quia numeros a, b et c, d inter se utcunque permutare licet, factores ipsius N quoque erunt $(a - d)^2 + (c - b)^2$ vel etiam, quia radices a, b, c, d negative assumere licet, $(a \pm c)^2 + (d \pm b)^2$ vel $(a \pm d)^2 + (c \pm b)^2$ seu harum formularum semisses aliaeve partes aliquotae. Quare cum numeri plus uno modo in duo quadrata resolubilis factores adeo assignari possint, ille numerus certe non erit primus, sed compositus. Q. E. D.

COROLLARIUM 1

41. Cum igitur numerus $N = aa + bb = cc + dd$ sit compositus, erit huiusmodi $N = (pp + qq)(rr + ss)$. Hinc autem vicissim duplex resolutio in duo quadrata resultat; erit nempe

$$a = pr + qs, \quad b = ps - qr$$

et

$$c = ps + qr, \quad d = pr - qs.$$

Hincque ulterius obtinetur $a - d = 2qs$ et $c - b = 2qr$, unde fit $\frac{r}{s} = \frac{c - b}{a - d}$. Quare si fractio $\frac{c - b}{a - d}$ ad minimos terminos reducatur, ut sit $\frac{c - b}{a - d} = \frac{r}{s}$, ex hac fractione $\frac{r}{s}$ orietur numeri N divisor $= rr + ss$, nisi sit par; nam si fuerit par, eius dimidium sumi debet.

COROLLARIUM 2

42. Simili modo, cum numeros a, b et c, d inter se permutare atque adeo negativos ponere liceat, si fractionum harum $\frac{a \pm c}{b \pm d}$ vel $\frac{a \pm d}{b \pm c}$ altera ad minimos terminos reducatur, ut fiat $= \frac{r}{s}$, erit $rr + ss$ semper divisor numeri propositi N.

COROLLARIUM 3

43. Quanquam autem hinc plures duobus divisores nasci videntur, tamen diversae formulae ita ad eundem divisorem deducunt, ut non plures quam duo eliciantur, siquidem numerus propositus duobus tantum modis in duo quadrata fuerit resolubilis. Sic si $N = 85 = 9^2 + 2^2 = 7^2 + 6^2$, formulae $\frac{9 \pm 7}{6 \pm 2}$, $\frac{9 \pm 6}{7 \pm 2}$ has quatuor tantum fractiones in minimis terminis suppeditant, nempe $\frac{2}{1}$, $\frac{4}{1}$, $\frac{5}{3}$, $\frac{3}{1}$, quarum binae posteriores pro formula $rr + ss$ duplum valorem tantum exhibent eius, qui ex primis oritur; unde patebit factores esse binos $2^2 + 1 = 5$ et $4^2 + 1 = 17$. Brevissime ergo hi factores inveniuntur, si tantum radices quadratorum pares et impares seorsim invicem combinentur et combinatio parium cum imparibus penitus omittatur, quia hinc fractiones orientur numeratorem et denominatorem impares habentes.

PROBLEMA

44. *Proposito numero quocunque formae* $4n + 1$ *explorare, utrum primus sit necne.*

SOLUTIO

Per operationem deinceps explicandam investigetur numerus propositus, utrum in duo quadrata resolvi possit necne, et si possit, an plus uno modo resolutio succedat. Si enim resolutionem in duo quadrata plane non admittat, id per § 32 certum erit signum numerum propositum non esse primum, etiamsi haec conclusio ex Propositione 5 non satis demonstrata sequatur. Hoc quidem casu de eius divisoribus nihil constat; interim tamen certo colligimus eum divisores primos habere formae $4m - 1$, quia, si omnes eius factores essent formae $4m + 1$, is certe in duo quadrata foret resolubilis. At si numerus propositus unico modo sit in duo quadrata resolubilis, tum infallibiliter pro primo erit habendus. Sin autem resolutio plus uno modo succedat, tum non solum constabit eum non esse primum, sed etiam eius divisores assignari poterunt per § 43. His perpensis regulam tradam, cuius ope resolubilitas in duo quadrata non difficulter explorari poterit.

Numerus propositus desinet vel in 1 vel in 3 vel in 7 vel in 9; casum, quo in 5 desinit, hic omitto, quia divisor 5 tum est manifestus et indicat

numerum non esse primum. Deinde numeri quadrati incipiendo a maximis ipso numero proposito minoribus successive ab eo subtrahantur, ut pateat, utrum unquam numerus quadratus restet; quoties enim hoc evenit, toties resolutio in duo quadrata succedit.

At cum numeri quadrati in nullum horum numerorum 2, 3, 7, 8 desinere queant, subtractio eorum numerorum quadratorum, qui residua dant in hos numeros desinentia, omitti poterit. Hinc tantum opus est, ut a numero proposito ea quadrata subtrahantur, quae residua in 0, 1, 4, 5, 6, 9 desinentia praebent; nempe,

si numerus propositus desinat in	quadrata subtrahenda desinent in	et horum quadratorum radices desinent in
1	0, 1, 5, 6	0, 1, 4, 5, 6, 9
3	4, 9	2, 3, 7, 8
7	1, 6	1, 4, 6, 9
9	0, 4, 5, 9	0, 2, 3, 5, 7, 8.

Pro quolibet igitur numero proposito $4n+1=N$ tot operationes seorsim instituantur, quot radicum idoneae sunt terminationes. Sit igitur pp maximum quadratum huius indolis, quod a numero proposito N subtrahi debet; ac tum successive subtrahantur quadrata $(p-10)^2$, $(p-20)^2$, $(p-30)^2$, $(p-40)^2$ etc. Verum residua hinc emergentia expedite per continuam additionem inveniri poterunt hoc modo:

Numerus propositus	N
a quo subtrahatur	pp
	$N-pp$
Addatur	$20p-100$
	$N-(p-10)^2$
Addatur	$20p-300$
	$N-(p-20)^2$
Addatur	$20p-500$
	$N-(p-30)^2$.

Numeri igitur successive addendi sunt

$$20p - 100, \quad 20p - 300, \quad 20p - 500, \quad 20p - 700 \quad \text{etc.},$$

qui decrescunt in ratione arithmetica per differentiam -200. Huiusmodi operatio pro singulis numeris p, quorum quadrata numero proposito proxime sunt minora et qui desinunt in aliquem figurarum supra indicatarum, instituatur neque ulterius continuetur, quam donec ad semissem numeri propositi N perveniatur. Si enim numerus N fuerit summa duorum quadratorum, alterum certe semissi ipsius minus sit necesse est. Quo observato, quot hac operatione prodibunt quadrata, tot modis numerus propositus in duo quadrata erit resolubilis.

Hanc autem operationem non admodum esse molestam omnibusque aliis methodis numeros primos explorandi longe anteferendam sequentia exempla declarabunt.

EXEMPLUM 1

45. *Explorare, utrum hic numerus* 82421 *primus sit necne.*

Operatio per sex columnas sequentes instituetur:

p	82421	p	82421	p	82421	p	82421	p	82421	p	82421
286	81796	285	81225	284	80656	281	78961	280	78400	279	77841
	□ 625		1196		1765		3460		4021		4580
	5620		5600		5580		5520		5500		5480
	6245		6796		7345		8980		9521		10060
	5420		5400		5380		5320		5300		5280
	11665		12196		12725		14300		14821		15340
	5220		5200		5180		5120		5100		5080
	16885		17396		17905		19420		19921		20420
	5020		5000		4980		4920		4900		4880
	21905		22396		22885		24340		24821		25300
	4820		4800		4780		4720		4700		4680
	26725		27196		27665		29060		29521		29980
	4620		4600		4580		4520		4500		4480
	31345		31796		32245		33580		34021		34460
	4420		4400		4380		4320		4300		4280
	35765		36196		36625		37900		38321		38740
	4220		4200		4180		4120		4100		4080
	39985		40396		40805		42020		42421		42820

Cum igitur hic unicum occurrat quadratum 625 ideoque numerus propositus 82421 unico modo sit in duo quadrata resolubilis, nempe $= 25^2 + 286^2$, is erit primus.

SCHOLION

46. In hoc computo quatuor columnae, ubi numeri residui desinunt vel in 5 vel in 0, notabiliter contrahi possunt omittendis omnibus iis, qui non desinunt vel in 25 vel in 00. Quare in columnis, in quibus residua desinunt vel in 5 vel in 0, subtrahatur primo proximum quadratum, quod residuum praebet vel in 25 vel in 00 desinens, hocque quadratum dicatur pp, ut residuum sit $= N - pp$; tum quadrata, unde residua simili modo desinentia oriuntur, erunt $(p-50)^2$, $(p-100)^2$, $(p-150)^2$ etc. ideoque haec residua obtinebun-

tur, si ad $N-pp$ continuo addantur hi numeri $100p-2500$, $100p-7500$, $100p-12500$[1]), qui decrescunt arithmetice secundum differentiam constantem 5000; unde hae columnae mox ad finem perducentur, dum eas non ultra semissem numeri propositi continuari opus est. Hoc igitur compendium locum habebit in numeris vel in 1 vel in 9 desinentibus, qui propterea, etiamsi sex columnas requirant, dum pro reliquis quatuor sufficiunt, facilius expedientur.

EXEMPLUM 2

47. *Explorare, utrum hic numerus* 100981 *primus sit necne.*

p 100981	p 100981	p 100981	p 100981
316 99856	315 99225	309 95481	310 96100
1125	1756	5500	4881
29100	6200	28400	6100
30225	7956	33900	10981
24100	6000	23400	5900
54325	13956	57300	16881
	5800		5700
p 100981	19756	p 100981	22581
284 80656	5600	291 84681	5500
20325	25356	16300	28081
25900	5400	26600	5300
$215^2=46225$	30756	42900	33381
	5200	21600	5100
	35956	64500	38481
	5000		4900
	40956		43381
	4800		4700
	45756		48081
	4600		
	50356		

Cum ergo unicum occurrat quadratum $46225=215^2$, unde fit $100981=215^2+234^2$, erit hic numerus primus.

1) Editio princeps (atque etiam *Comment. arithm.*): *hi numeri* $100p-2500$; $100p-17500$; $100p-125000$ *qui* ... Correxit F. R.

EXEMPLUM 3

48. *Explorare, utrum hic numerus* 1000009 *sit primus necne.*[1])

p	1000009	
1000	1000000	
$3^2 =$	9	277509
	19900	16900
	19909	294409
	19700	16700
	39609	311109
	19500	16500
	59109	327609
	19300	16300
	78409	343909
	19100	16100
	97509	360009
	18900	15900
	116409	375909
	18700	15700
	135109	391609
	18500	15500
	153609	407109
	18300	15300
	171909	422409
	18100	15100
	190009	437509
	17900	14900
	207909	452409
	17700	14700
	225609	467109
	17500	14500
	243109	481609
	17300	14300
	260409	495909
	17100	
	277509	

p	1000009
978	956484
	43525
	95300
	138825
	90300
	229125
	85300
	314425
	80300
	394725
	75300
	470025

p	1000009
972	944784
$235^2 =$	55225
	94700
	149925
	89700
	239625
	84700
	324325
	79700
	404025
	74700
	478725

p	1000009
997	994009
	6000
	97200
	103200
	92200
	195400
	87200
	282600
	82200
	364800
	77200
	442000

p	1000009
953	908209
	91800
	92800
	184600
	87800
	272400
	82800
	355200
	77800
	433000

p	1000009	
995	990025	
	9984	285984
	19800	16800
	29784	302784
	19600	16600
	49384	319384
	19400	16400
	68784	335784
	19200	16200
	87984	351984
	19000	16000
	106984	367984
	18800	15800
	125784	383784
	18600	15600
	144384	399384
	18400	15400
	162784	414784
	18200	15200
	180984	429984
	18000	15000
	198984	444984
	17800	14800
	216784	459784
	17600	14600
	234384	474384
	17400	14400
	251784	488784
	17200	
	268984	
	17000	
	285984	

Hic ergo numerus 1000009 duplici modo est in duo quadrata resolubilis,

1) Sequentis computi errores, qui in editione principe inveniuntur, iam in *Comment. arithm.* correcti sunt. F. R.

quippe $= 1000^2 + 3^2 = 235^2 + 972^2$, unde is non erit primus; factores vero eius reperientur ex hac formula $\frac{1000 \pm 972}{235 \pm 3}$ ad minimos terminos reducta, unde oritur:

$$\frac{1000+972}{235+3} = \frac{1972}{238} \overset{2}{\smile} \frac{986}{119} \overset{17}{\smile} \frac{58}{7}, \text{ ergo factor } = 3413,$$

$$\frac{1000+972}{235-3} = \frac{1972}{232} \overset{4}{\smile} \frac{493}{58} \overset{29}{\smile} \frac{17}{2}, \text{ ergo factor } = 293;$$

qui factores facilius invenientur ex formula

$$\frac{1000-972}{235 \pm 3} = \frac{28}{238} = \frac{14}{119} = \frac{2}{17} \quad \text{et} \quad \frac{28}{232} = \frac{7}{58}.$$

Novimus ergo esse $1000009 = 293 \cdot 3413$, qui factores nulla alia methodo tam facile reperti fuissent.

EXEMPLUM 4

49. *Explorare, utrum hic numerus* 233033 *primus sit necne.*

233033	233033	233033	233033
$482^2 = 232324$	$477^2 = 227529$	$473^2 = 223729$	$478^2 = 228484$
709	5504	9304	4549
9540	9440	9360	9460
10249	14944	18664	14009
9340	9240	9160	9260
19589	24184	27824	23269
9140	9040	8960	9060
28729	33224	36784	32329
8940	8840	8760	8860
37669	42064	45544	41189
8740	8640	8560	8660
46409	50704	54104	49849
8540	8440	8360	8460
54949	59144	62464	58309
8340	8240	8160	8260
63289	67384	70624	66569
8140	8040	7960	8060
71429	75424	78584	74629
7940	7840	7760	7860
79369	83264	86344	82489
7740	7640	7560	7660
87109	90904	93904	90149
7540	7440	7360	7460
94649	98344	101264	97609
7340	7240	7160	7260
101989	105584	108424	104869
7140	7040	6960	7060
109129	112624	115384	111929
6940	6840	6760	6860
116069	119464	122144	118789

Quia ergo hic numerus, etsi est formae $4n+1$, non est summa duorum quadratorum, vi Propositionis 5 colligimus eum non esse numerum primum. Factores quidem eius hinc assignare non licet, interim tamen concludimus eum saltem duos habere factores formae $4m-1$; qui investigatione instituta reperientur $467 \cdot 499$.

EXEMPLUM 5

50. *Explorare, utrum hic numerus 262657 primus sit necne.*

262657	262657	262657	262657
$511^2 = 261121$	$509^2 = 259081$	$506^2 = 256036$	$504^2 = 254016$
1536	3576	6621	8641
10120	10080	10020	9980
11656	13656	$129^2 = 16641$	18621
9920	9880	9820	9780
21576	23536	26461	28401
9720	9680	9620	9580
31296	33216	36081	37981
9520	9480	9420	9380
40816	42696	45501	47361
9320	9280	9220	9180
50136	51976	54721	56541
9120	9080	9020	8980
59256	61056	63741	65521
8920	8880	8820	8780
68176	69936	72561	74301
8720	8680	8620	8580
76896	78616	81181	82881
8520	8480	8420	8380
85416	87096	89601	91261
8320	8280	8220	8180
93736	95376	97821	99441
8120	8080	8020	7980
101856	103456	105841	107421
7920	7880	7820	7780
109776	111336	113661	115201
7720	7680	7620	7580
117496	119016	121281	122781
7520	7480	7420	7380
125016	126496	128701	130161
7320	7280	7220	7180
132336	133776	135921	137341

Cum igitur hic unicum quadratum occurrat $16641 = 129^2$, ita ut sit unico modo $262657 = 129^2 + 496^2$, hique numeri 129 et 496 sint inter se primi, certum est numerum 262657 esse primum.

EXEMPLUM 6

51. *Explorare, utrum hic numerus* 32129 *sit primus necne.*

32129	32129	32129	32129
$152^2 = 23104$	$177^2 = 31329$	$175^2 = 30625$	$170^2 = 28900$
$95^2 =$ 9025	800	1504	3229
12700	15200	3400	3300
21725	16000	4904	6529
		3200	3100
32129	32129	8104	9629
$148^2 = 21904$	$173^2 = 29929$	3000	2900
10225	2200	11104	12529
12300	14800	2800	2700
22525	17000	13904	15229
		2600	2500
		16504	17729

Hic igitur numerus quoque unico modo est in duo quadrata resolubilis $= 95^2 + 152^2$, sed quia hi numeri 95 et 152 non sunt primi inter se, sed communem divisorem habent 19, numerus propositus non erit primus, sed factorem habet $19^2 = 361$ estque $32129 = 19^2 \cdot 89$.

SCHOLION

52. Quanquam haec methodus explorandi numeros, utrum sint primi necne, tantum ad numeros in hac forma $4n + 1$ contentos extenditur, tamen saepenumero in diiudicandis numeris magnum subsidium afferre potest. Quantum autem aliis regulis hoc idem praestandi antecellat, quilibet, qui periculum huius rei facere velit, facile experietur. Qui enim numerum millione non minorem via consueta examinare voluerit, eius divisionem per omnes numeros primos ad millenarium usque tentare debet, quod opus intra plures horas non absolvet, dum ope huius regulae ipsi vix semihora opus erit.

DEMONSTRATIO THEOREMATIS FERMATIANI OMNEM NUMERUM PRIMUM FORMAE $4n+1$ ESSE SUMMAM DUORUM QUADRATORUM[1]

Commentatio 241 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 5 (1754/5), 1760, p. 3—13
Summarium ibidem p. 3—5

SUMMARIUM

De hoc insigni theoremate iam in superiori tomo[2] a Cel. Auctore egregiae observationes sunt prolatae, quibus eius veritas tam solidis rationibus fuit comprobata, ut nullum dubium relinqui videretur; neque tamen hae rationes vicem firmae demonstrationis sustinebant. In hoc memorabile cernitur exemplum eiusmodi propositionis, de cuius veritate dubitare nefas sit, etiamsi completa demonstratione destituamur. Talibus autem propositionibus nusquam minus quam in Mathesi locum relinqui vulgo putatur, ubi omnia firmissimis demonstrationibus munita videntur. Verum hoc etiam tantum in doctrina numerorum usu venire deprehendimus, in quorum natura scrutanda FERMATIUS ita excelluit, ut quam plurimas proprietates detexerit atque etiam demonstrasse sit professus, quarum plerasque etiamnunc sine demonstratione veritati consentaneas agnoscere debemus; dum in reliquis Matheseos partibus ac multo magis in aliis scientiae generibus, quarum propositionum veritas non per rigidas demonstrationes nobis est perspecta, eae merito suspectae videri debent, cum adeo plerumque, quandoquidem eas accuratius intueri licet, falsae deprehenduntur. In eo genere igitur imprimis istud theorema FERMATIANUM, quod omnis numerus primus formae $4n+1$

1) Demonstrationem hac in Commentatione 241 contentam EULERUS iam in epistola d. 12. Apr. 1749 ad CHR. GOLDBACH scripta exposuit, *Correspondance math. et phys. publiée par P. H. Fuss*, St.-Pétersbourg 1843, t. I, p. 493; *LEONHARDI EULERI Opera omnia*, series III. F. R.

2) Vide Commentationem 228 huius voluminis. F. R.

sit summa duorum quadratorum, studium Geometrarum fatigavit atque Auctor noster[1]) in eius demonstratione investiganda multum diuque desudasse videtur, cum in superiori tomo plura theoremata huc pertinentia ex profundissimis numerorum mysteriis elicuisset neque tamen scopum attingere potuisset. Tam prope autem eo pertigerat, ut hic quasi reliquo spatio feliciter confecto tandem perfectam demonstrationem sit adeptus, quae, cum per tot ambages tantasque numerorum difficultates sit deducta, eo magis attentionem et studium Geometrarum excitare debebit. Nullum enim dubium est, quin his argumentis probe perpensis via multo brevior et planior eodem perveniendi aperiatur. Talis autem demonstratio brevior ac certe nobis planior aditum ad abscondita numerorum arcana esset patefactura, quae etiamnum nonnisi quasi per tenebras contemplari licet.

Versatur ergo memorabile theorema circa numeros formae $4n+1$ seu eos numeros impares, qui unitate excedunt multipla quaternarii; qui sunt 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49 etc. In his distinguuntur numeri primi 5, 13, 17, 29, 37, 41 a compositis 9, 21, 25, 33, 45, 49 ac de illis affirmatur singulos esse aggregata binorum quadratorum, veluti $5=1+4$, $13=4+9$, $17=1+16$, $29=4+25$, $37=1+36$, $41=16+25$ etc., quod eo magis mirum videtur, cum haec quadrata nulla ratione procedant. Inter compositos autem etsi alii ipsi sunt quadrata, ut 9, 25, 49 etc., alii vero etiam summae duorum quadratorum, ut $45=9+36$, tamen inter eos dantur, ut 21, 33, qui nullo modo summae duorum quadratorum[2]) aequantur, unde propositio tantum ad numeros primos formae $4n+1$ restringitur. Huius ergo veritas nunc demum pro demonstrata est habenda, siquidem demonstratio Fermatiana penitus intercidit. In praecedente autem tomo demonstratio eo erat producta, ut ostenderetur, quoties $4n+1$ sit numerus primus, semper dari eiusmodi duos numeros a et b, ut $a^{2n}+b^{2n}$ esset per $4n+1$ divisibile; hoc ipsum autem tum sine probatione relinquebatur. Nunc igitur negotium ita Auctor absolvit, ut, cum multo ante demonstrasset hanc formam $a^{4n}-b^{4n}$ seu productum hoc $(a^{2n}-b^{2n})(a^{2n}+b^{2n})$ semper esse per numerum primum $4n+1$ divisibile, doceret semper dari casus, quibus alter factor $a^{2n}-b^{2n}$ non sit divisibilis per $4n+1$; tum enim necessario sequitur alterum factorem $a^{2n}+b^{2n}$ hunc divisorem complecti. Quod reliquum est, iam ante erat praestitum; quia enim $a^{2n}+b^{2n}$ est summa duorum quadratorum simulque firma demonstratione evictum est summam talium binorum quadratorum nullos alios divisores admittere, nisi qui ipsi sint duorum quadratorum summae, necesse est numerum $4n+1$ esse summam duorum quadratorum. Hinc igitur liquet, quam subtilia et undequaque conquisita ratiocinia ad huiusmodi demonstrationes requirantur et quam longe adhuc a solida numerorum cognitione simus remoti.

1) Secundum manuscriptum; editio princeps: *Cel. Eulerus.* F. R.

2) In editione principe manuscripti verba *ut $45=9+36$, tamen . . . quadratorum* omissa sunt. F. R.

1. Cum nuper[1]) eos essem contemplatus numeros, qui ex additione duorum quadratorum oriuntur, plures demonstravi proprietates, quibus tales numeri sunt praediti; neque tamen meas meditationes eousque perducere licuit, ut huius theorematis, quod FERMATIUS[2]) olim Geometris demonstrandum proposuit, veritatem solide ostendere potuissem. Tentamen[3]) tamen demonstrationis tum exposui, unde certitudo huius theorematis multo luculentius elucet, etiamsi criteriis rigidae demonstrationis destituatur, neque dubitavi, quin iisdem vestigiis insistendo tandem demonstratio desiderata facilius obtineri possit; quod quidem ex eo tempore mihi ipsi usu venit, ita ut tentamen illud, si alia quaedam levis consideratio accedat, in rigidam demonstrationem abeat. Nihil quidem novi in hac re me praestitisse gloriari possum, cum ipse FERMATIUS iam demonstrationem huius theorematis elicuisse se profiteatur; verum quod eam nusquam publici iuris fecit, eius iactura perinde ac plurimorum aliorum egregiorum huius viri inventorum efficit, ut, quae nunc demum de his deperditis rebus quasi recuperamus, ea non immerito pro novis inventis habeantur. Cum enim nemo unquam tam feliciter in arcana numerorum penetraverit quam FERMATIUS, omnis opera in hac scientia ulterius excolenda frustra impendi videtur, nisi ante, quae ab hoc excellenti Viro iam fuerunt investigata, quasi de novo in lucem protrahantur. Etsi enim post eum plures Viri docti in hoc studiorum genere vires suas exercuerunt, nihil tamen plerumque sunt consecuti, quod cum ingenio huius Viri comparari posset.

2. Ut autem demonstrationem theorematis, quod hic considero, instituam, duas propositiones in subsidium vocari oportet, quarum demonstrationem iam alibi dedi. Altera est, quod omnes numeri, qui sunt divisores summae duorum quadratorum inter se primorum, ipsi sint summae duorum quadratorum; sic si a et b sint numeri inter se primi atque numeri ex iis formati $aa+bb$ divisor sit d, erit quoque d summa duorum quadratorum; huius theorematis demonstrationem dedi in scripto ante memorato, quo numeros, qui sunt duorum quadratorum summae, sum contemplatus.[4]) Altera propositio, qua demonstratio sequens indiget, ita se habet: Si p sit numerus primus atque

1) Vide Commentationem 228 huius voluminis. F. R.
2) Vide notam 2 p. 310. F. R.
3) Vide p. 311. F. R.
4) Vide Commentationem 228 huius voluminis, imprimis propositionem 4. F. R.

a et b numeri quicunque per p non divisibiles, erit semper $a^{p-1}-b^{p-1}$ per numerum primum p divisibilis; demonstrationem huius rei iam dudum in Nov. comment. acad. Petrop. tom. I[1]) dedi.

3. Quodsi iam $4n+1$ sit numerus primus, per eum omnes numeri in hac forma $a^{4n}-b^{4n}$ contenti erunt divisibiles, siquidem neuter numerorum a et b seorsim per $4n+1$ fuerit divisibilis. Quare si a et b sint numeri minores quam $4n+1$ (cyphra tamen excepta), numerus inde formatus $a^{4n}-b^{4n}$ sine ulla limitatione per numerum primum propositum $4n+1$ erit divisibilis. Cum autem $a^{4n}-b^{4n}$ sit productum horum factorum $a^{2n}+b^{2n}$ et $a^{2n}-b^{2n}$, necesse est, ut alteruter horum factorum sit per $4n+1$ divisibilis; fieri enim nequit, ut vel neuter vel uterque simul divisorem habeat $4n+1$. Quodsi iam demonstrari posset dari casus, quibus forma $a^{2n}+b^{2n}$ sit divisibilis per $4n+1$, quoniam $a^{2n}+b^{2n}$ ob exponentem $2n$ parem est summa duorum quadratorum, quorum neutrum seorsim per $4n+1$ divisibile existit, inde sequeretur hunc numerum $4n+1$ esse summam duorum quadratorum.

4. Verum summa $a^{2n}+b^{2n}$ toties erit per $4n+1$ divisibilis, quoties differentia $a^{2n}-b^{2n}$ per eundem numerum non est divisibilis. Quare qui negaverit numerum primum $4n+1$ esse summam duorum quadratorum, is negare cogitur ullum numerum huius formae $a^{2n}+b^{2n}$ per $4n+1$ esse divisibilem; eundem propterea affirmare oportet omnes numeros in hac forma $a^{2n}-b^{2n}$ contentos per $4n+1$ esse divisibiles, siquidem neque a neque b per $4n+1$ sit divisibile. Quamobrem mihi hic demonstrandum est non omnes numeros in forma $a^{2n}-b^{2n}$ contentos per $4n+1$ esse divisibiles; hoc enim si praestitero, certum erit dari casus seu numeros pro a et b substituendos, quibus forma $a^{2n}-b^{2n}$ non sit per $4n+1$ divisibilis; illis ergo casibus altera forma $a^{2n}+b^{2n}$ necessario per $4n+1$ erit divisibilis. Unde, cum a^{2n} et b^{2n} sint numeri quadrati, conficietur id, quod proponitur, scilicet numerum $4n+1$ esse summam duorum quadratorum.

5. Ut igitur demonstrem non omnes numeros in hac forma $a^{2n}-b^{2n}$ contentos seu non omnes differentias inter binas potestates dignitatis $2n$ esse

1) Editio princeps: *in Comment. Acad. Petrop. Tom. VIII.* Commentatio autem commemorata est Commentatio 134 huius voluminis; vide ibidem theorema 4. F. R.

per $4n+1$ divisibiles, considerabo seriem harum potestatum ab unitate usque ad eam, quae a radice $4n$ formatur,

$$1, \; 2^{2n}, \; 3^{2n}, \; 4^{2n}, \; 5^{2n}, \; 6^{2n}, \; \ldots \; (4n)^{2n}$$

ac iam dico non omnes differentias inter binos terminos huius seriei esse per $4n+1$ divisibiles. Si enim singulae differentiae primae

$$2^{2n}-1, \quad 3^{2n}-2^{2n}, \quad 4^{2n}-3^{2n}, \quad 5^{2n}-4^{2n}, \; \ldots \; (4n)^{2n}-(4n-1)^{2n}$$

per $4n+1$ essent divisibiles, etiam differentiae huius progressionis, quae sunt differentiae secundae illius seriei, per $4n+1$ essent divisibiles; atque ob eandem rationem differentiae tertiae, quartae, quintae etc. omnes forent per $4n+1$ divisibiles ac denique etiam differentiae ordinis $2n$, quae sunt, ut constat, omnes inter se aequales. Differentiae autem ordinis $2n$ sunt $=1\cdot 2\cdot 3\cdot 4\cdots 2n$, quae ergo per numerum primum $4n+1$ non sunt divisibiles, ex quo vicissim sequitur ne omnes quidem differentias primas per $4n+1$ esse divisibiles.

6. Quo vis huius demonstrationis melius perspiciatur, notandum est differentiam ordinis $2n$ produci ex $2n+1$ terminis seriei propositae, qui, si ab initio capiantur, omnes ita sunt comparati, ut binorum quorumvis differentiae per $4n+1$ divisibiles esse debeant, si theorematis veritas negetur. Sin autem plures termini ad hanc differentiam ultimam constituendam concurrerent iique ultra terminum $(4n)^{2n}$ progrederentur, quoniam differentiae a termino sequente $(4n+1)^{2n}$ ortae ad enunciata theorematis non pertinent, demonstratio nullam vim retineret. Hinc autem, quod differentia ultima, quam sumus contemplati, tantum ab $2n+1$ terminis pendet, conclusio, quam inde deduximus, omnino est legitima; indeque sequitur dari differentias primas, veluti $a^{2n}-(a-1)^{2n}$, quae non sint per $4n+1$ divisibiles atque ita quidem, ut a non sit maior quam $2n+1$. Hinc autem porro recte infertur summam $a^{2n}+(a-1)^{2n}$ ideoque summam duorum quadratorum per $4n+1$ necessario esse divisibilem ideoque numerum primum $4n+1$ summam esse duorum quadratorum.

7. Quoniam differentia ordinis $2n$ ab $2n+1$ terminis seriei potestatum pendet, totidem tantum ab initio captos consideremus

$$1, \; 2^{2n}, \; 3^{2n}, \; 4^{2n}, \; 5^{2n}, \; 6^{2n}, \; \ldots \; (2n)^{2n}, \quad (2n+1)^{2n},$$

unde differentiae primae erunt

$$2^{2n}-1,\quad 3^{2n}-2^{2n},\quad 4^{2n}-3^{2n},\quad 5^{2n}-4^{2n},\ \ldots\ (2n+1)^{2n}-(2n)^{2n},$$

cuius progressionis terminorum numerus est $=2n$. Ex demonstratione itaque praecedente patet non omnes terminos huius progressionis differentiarum esse per numerum primum $4n+1$ divisibiles; neque tamen hinc intelligimus, quot et quinam sint illi termini per $4n+1$ non divisibiles. Ad demonstrationem enim sufficit, si vel unicus terminus, quisquis ille sit, per $4n+1$ non sit divisibilis. Quodsi autem casus speciales evolvamus, quibus $4n+1$ est numerus primus, ex differentiis istis, quarum numerus est $2n$, reperiemus semper semissem esse per $4n+1$ divisibilem, alterum vero semissem non divisibilem; quae observatio etsi ad vim demonstrationis non spectat, tamen ad eam illustrandam non parum confert, quare aliquot casus speciales ad examen revocasse iuvabit.

8. Minimus numerus primus formae $4n+1$ est $=5$, qui oritur, si $n=1$; unde duae habebuntur differentiae 2^2-1 et 3^2-2^2, quarum prior non est divisibilis per 5, altera vero est divisibilis. Pro reliquis casibus utamur signo d ad eas differentias indicandas, quae sunt divisibiles, at signo 0 eas notemus, quae non sunt divisibiles; quae signa differentiis pro quovis casu subscribamus:

$4n+1$	Differentiae							
13	2^6-1,	3^6-2^6,	4^6-3^6,	5^6-4^6,	6^6-5^6,	7^6-6^6		
	0	0	d	0	d	d		
17	2^8-1,	3^8-2^8,	4^8-3^8,	5^8-4^8,	6^8-5^8,	7^8-6^8,	8^8-7^8,	9^8-8^8
	d	0	0	0	d	d	0	d
29	$2^{14}-1$,	$3^{14}-2^{14}$,	$4^{14}-3^{14}$,	$5^{14}-4^{14}$,	$6^{14}-5^{14}$,	$7^{14}-6^{14}$,	$8^{14}-7^{14}$,	$9^{14}-8^{14}$,
	0	d	0	d	d	d	0	0
	$10^{14}-9^{14}$,	$11^{14}-10^{14}$,	$12^{14}-11^{14}$,	$13^{14}-12^{14}$,	$14^{14}-13^{14}$,	$15^{14}-14^{14}$		
	0	d	d	0	0	d		

Hinc patet terminos divisibiles et non divisibiles nulla certa lege contineri, etiamsi utrique sint multitudine pares; tamen per se est perspicuum ultimum terminum $(2n+1)^{2n}-(2n)^{2n}$ semper per $4n+1$ esse divisibilem, quia factorem habet $(2n+1)^2-4nn=4n+1$; at de reliquis nihil certi statui potest.

9. Porro quoque ad vim demonstrationis penitius perspiciendam notari oportet demonstrationem tum solum locum habere, si numerus $4n+1$ sit primus, prorsus uti natura theorematis postulat. Nam si $4n+1$ non esset numerus primus, neque de eo affirmari posset, quod sit summa duorum quadratorum, neque forma $a^{4n}-b^{4n}$ per eum esset necessario divisibilis. Quin etiam ultima conclusio foret falsa, qua pronunciavimus differentias illas ordinis $2n$, quae sunt $1\cdot 2\cdot 3\cdot 4\cdots 2n$, non esse per $4n+1$ divisibiles. Si enim $4n+1$ non esset numerus primus, sed factores haberet, qui essent minores quam $2n$, tum utique productum $1\cdot 2\cdot 3\cdot 4\cdots 2n$ hos factores contineret foretque idcirco per $4n+1$ divisibile. At si $4n+1$ est numerus primus, tum demum affirmare licet productum $1\cdot 2\cdot 3\cdot 4\cdots 2n$ plane non esse per $4n+1$ divisibile, quia hoc productum per nullos alios numeros dividi potest, nisi qui tanquam factores in illud ingrediuntur.

10. Cum denique demonstratio tradita hoc nitatur fundamento, quod seriei potestatum 1, 2^{2n}, 3^{2n}, 4^{2n} etc. differentiae ordinis $2n$ sint constantes omnesque $=1\cdot 2\cdot 3\cdot 4\cdots 2n$, hoc uberius explicandum videtur, etsi passim in libris analyticorum solide expositum reperitur.[1]) Primum igitur notandum est, si seriei cuiuscunque terminus generalis seu is, qui exponenti indefinito x respondet, sit $=Ax^m+Bx^{m-1}+Cx^{m-2}+Dx^{m-3}+Ex^{m-4}+$ etc., hanc seriem ad gradum m referri, quia m est exponens maximae potestatis ipsius x. Deinde si hic terminus generalis a sequente $A(x+1)^m+B(x+1)^{m-1}+C(x+1)^{m-2}+$ etc. subtrahatur, prodibit terminus generalis seriei differentiarum, in quo exponens summae potestatis ipsius x erit $=m-1$, ideoque series differentiarum ad gradum inferiorem $m-1$ pertinebit. Pari modo ex termino generali seriei differentiarum primarum colligetur terminus generalis seriei differentiarum secundarum, qui igitur denuo ad gradum depressiorem $m-2$ pertinebit.

11. Ita si series proposita ad gradum m referatur, series differentiarum primarum ad gradum $m-1$ referetur, series porro differentiarum secundarum ad gradum $m-2$, series differentiarum tertiarum ad gradum $m-3$, series differentiarum quartarum ad gradum $m-4$ et in genere series differentiarum ordinis n ad gradum $m-n$ pertinebit. Unde series differentiarum

---

1) Vide exempli gratia L. EULERI *Institutiones calculi differentialis*, partis prioris cap. I et II imprimis § 50 et 51, Petropoli 1755; *LEONHARDI EULERI Opera omnia*, series I, vol. 10. F. R.

ordinis m ad gradum $m-m=0$ perveniet eiusque ergo terminus generalis, quia summa ipsius x potestas est $=x^0=1$, erit quantitas constans ideoque omnes differentiae ordinis m inter se erunt aequales. Hinc serierum primi gradus, quarum terminus generalis est $=Ax+B$, iam differentiae primae sunt inter se aequales, serierum autem secundi gradus, quae hoc termino generali Ax^2+Bx+C continentur, differentiae secundae sunt aequales, et ita porro.

12. Quodsi ergo seriem quamcunque potestatum consideremus

$$1, \quad 2^m, \quad 3^m, \quad 4^m, \quad 5^m, \quad 6^m, \quad 7^m, \quad 8^m \quad \text{etc.},$$

cuius terminus generalis est $=x^m$ seu is, qui indici x respondet, series differentiarum ordinis m ex terminis inter se aequalibus constabit. At seriei differentiarum primarum terminus generalis erit

$$(x+1)^m - x^m;$$

qui a sequente $(x+2)^m-(x+1)^m$ subtractus dabit terminum generalem seriei differentiarum secundarum, qui erit

$$(x+2)^m - 2(x+1)^m + x^m.$$

Hinc porro seriei differentiarum tertiarum erit terminus generalis

$$(x+3)^m - 3(x+2)^m + 3(x+1)^m - x^m;$$

ac tandem seriei differentiarum ordinis m concluditur terminus generalis

$$(x+m)^m - m(x+m-1)^m + \frac{m(m-1)}{1\cdot 2}(x+m-2)^m$$
$$-\frac{m(m-1)(m-2)}{1\cdot 2\cdot 3}(x+m-3)^m + \text{etc.};$$

qui cum sit quantitas constans, idem erit, quicunque numerus pro x substituatur; erit ergo vel

$$m^m - m(m-1)^m + \frac{m(m-1)}{1\cdot 2}(m-2)^m - \frac{m(m-1)(m-2)}{1\cdot 2\cdot 3}(m-3)^m + \text{etc.}$$

vel

$$(m+1)^m - mm^m + \frac{m(m-1)}{1\cdot 2}(m-1)^m - \frac{m(m-1)(m-2)}{1\cdot 2\cdot 3}(m-2)^m + \text{etc.},$$

ubi in forma priori posuimus $x=0$, in posteriori $x=1$.

13. Evolvamus iam casus huius seriei speciales et a potestatibus minimis ad altiores ascendamus. Ac posito primo $m = 1$ seriei 1, 2, 3, 4, 5, 6 etc. terminus generalis differentiarum primarum erit

$$\text{vel}\quad 1^1 - 1\cdot 0^1 = 1 \quad\text{vel}\quad 2^1 - 1\cdot 1^1 = 1.$$

Si $m = 2$, seriei 1, 2^2, 3^2, 4^2, 5^2 etc. differentiae secundae sunt

$$\text{vel}\quad 2^2 - 2\cdot 1^2 \quad\text{vel}\quad 3^2 - 2\cdot 2^2 + 1\cdot 1^2;$$

at est $2^2 - 2\cdot 1^2 = 2(2^1 - 1\cdot 1^1)$, unde hae differentiae secundae sunt

$$= 2\cdot 1.$$

Sit $m = 3$ et seriei 1, 2^3, 3^3, 4^3, 5^3 etc. differentiae tertiae erunt

$$\text{vel}\quad 3^3 - 3\cdot 2^3 + 3\cdot 1^3 \quad\text{vel}\quad 4^3 - 3\cdot 3^3 + 3\cdot 2^3 - 1\cdot 1^3;$$

at

$$3^3 - 3\cdot 2^3 + 3\cdot 1^3 = 3(3^2 - 2\cdot 2^2 + 1\cdot 1^2) = 3\cdot 2\cdot 1,$$

quia ex casu praecedente est $3^2 - 2\cdot 2^2 + 1\cdot 1^2 = 2\cdot 1$. Simili modo, si $m = 4$, seriei 1, 2^4, 3^4, 4^4, 5^4 etc. differentiae quartae erunt

$$\text{vel}\quad 4^4 - 4\cdot 3^4 + 6\cdot 2^4 - 4\cdot 1^4 \quad\text{vel}\quad 5^4 - 4\cdot 4^4 + 6\cdot 3^4 - 4\cdot 2^4 + 1\cdot 1^4;$$

at est

$$4^4 - 4\cdot 3^4 + 6\cdot 2^4 - 4\cdot 1^4 = 4(4^3 - 3\cdot 3^3 + 3\cdot 2^3 - 1\cdot 1^3) = 4\cdot 3\cdot 2\cdot 1.$$

14. Quo hic progressus melius perspiciatur, sint seriei 1, 2^m, 3^m, 4^m, 5^m etc. differentiae ordinis $m = P$, seriei 1, 2^{m+1}, 3^{m+1}, 4^{m+1}, 5^{m+1} etc. differentiae ordinis $m+1 = Q$; erit

$$P = (m+1)^m - mm^m + \frac{m(m-1)}{1\cdot 2}(m-1)^m - \frac{m(m-1)(m-2)}{1\cdot 2\cdot 3}(m-2)^m + \text{etc.},$$

$$Q = (m+1)^{m+1} - (m+1)m^{m+1} + \frac{(m+1)m}{1\cdot 2}(m-1)^{m+1} - \frac{(m+1)m(m-1)}{1\cdot 2\cdot 3}(m-2)^{m+1} + \text{etc.},$$

ubi P ex forma posteriori, at Q ex forma priori expressimus. Hic primo patet in utraque expressione parem esse terminorum numerum et singulos terminos expressionis P esse ad singulos terminos expressionis Q uti 1 ad

$m+1$. Namque est

$$(m+1)^m : (m+1)^{m+1} = 1 : m+1,$$

$$mm^m : (m+1)m^{m+1} = 1 : m+1,$$

$$\frac{m(m-1)}{1\cdot 2}(m-1)^m : \frac{(m+1)m}{1\cdot 2}(m-1)^{m+1} = 1 : m+1,$$

$$\frac{m(m-1)(m-2)}{1\cdot 2\cdot 3}(m-2)^m : \frac{(m+1)m(m-1)}{1\cdot 2\cdot 3}(m-2)^{m+1} = 1 : m+1$$

etc.

Hanc ob rem erit

$$P : Q = 1 : m+1 \quad \text{ideoque} \quad Q = (m+1)P.$$

15. Hinc ergo patet fore

seriei	differentias	
$1,\ 2,\ 3,\ 4,\ 5$ etc.	primas	$=1;$
$1,\ 2^2,\ 3^2,\ 4^2,\ 5^2$ etc.	secundas	$=1\cdot 2,$
$1,\ 2^3,\ 3^3,\ 4^3,\ 5^3$ etc.	tertias	$=1\cdot 2\cdot 3,$
$1,\ 2^4,\ 3^4,\ 4^4,\ 5^4$ etc.	quartas	$=1\cdot 2\cdot 3\cdot 4,$
$\vdots$	$\vdots$	
$1,\ 2^m,\ 3^m,\ 4^m,\ 5^m$ etc.	ordinis m	$=1\cdot 2\cdot 3\cdots m,$

ergo

$1,\ 2^{2n},\ 3^{2n},\ 4^{2n},\ 5^{2n}$ etc.	ordinis $2n$	$=1\cdot 2\cdot 3\cdots 2n.$

Atque ita quoque demonstravimus seriei potestatum $1, 2^{2n}, 3^{2n}, 4^{2n}, 5^{2n}$ etc. differentias ordinis $2n$ non solum esse constantes, sed etiam aequari producto $1\cdot 2\cdot 3\cdots 2n$, uti in demonstratione theorematis propositi assumsimus.

DEMONSTRATIO THEOREMATIS FERMATIANI OMNEM NUMERUM SIVE INTEGRUM SIVE FRACTUM ESSE SUMMAM QUATUOR PAUCIORUMVE QUADRATORUM[1]

Commentatio 242 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 5 (1754/5), 1760, p. 13—58
Summarium ibidem p. 6—7

SUMMARIUM

Huic scripto pag. 13 sine peculiari titulo adiungitur nova dissertatio, in qua residua, quae in divisione numerorum quadratorum per quosvis numeros remanent, examini subiiciuntur, unde iterum egregiae numerorum proprietates deducuntur, vel omnino novae vel iam quidem cognitae, sed novo modo demonstratae. Nemo ignorat omnes numeros quadratos, qui per 3 dividi nequeunt, in divisione semper unitatem relinquere neque ullum dari numerum quadratum, qui per 3 divisus duo relinquat. Simili modo nullus datur numerus quadratus, qui per 4 divisus vel 2 vel 3 relinquat, sed residuum semper est 1, nisi divisio succedat, quo casu residuum censendum est 0. Deinde nullus datur numerus quadratus, qui per 5 divisus relinquat 2 vel 3, sed residua semper sunt vel 0 vel 1 vel 4. Atque in genere per quemcunque numerum numeri quadrati dividantur, a residuis certi numeri excluduntur, quos Cel. Auctor hic imprimis considerat et *non-residua* appellat. Tum pro quocunque divisore eximias proprietates tam inter residua quam non-residua observat indeque plura egregia theoremata demonstrat; veluti nunquam evenire posse, ut haec forma $4mn-m-n$, quicunque etiam numeri pro m et n assumantur, fiat numerus quadratus. His speculationibus tantum non deducitur Auctor tandem ad illud elegantissimum theorema, *quod omnes numeri sint aggregata quatuor vel pauciorum quadratorum*, quod etiam

1) In editione principe (atque etiam in *Comment. arithm.*) titulus deest. Vide P. STÄCKEL und W. AHRENS, *Der Briefwechsel zwischen C. G. J. JACOBI und P. H. VON FUSS über die Herausgabe der Werke LEONHARD EULERS*, Leipzig 1908, p. 62, 63, 89 (imprimis notam 2) atque etiam p. 26 et 27. F. R.

FERMATIUS ex profundissimis numerorum mysteriis demonstrasse affirmat et cuius demonstrationis iactura aeque est dolenda ac tot veterum scriptorum, quibus nos temporum iniuria[1]) privavit. Etsi enim Auctor in postremo theoremate demonstrat *omnem numerum esse summam quatuor quadratorum vel pauciorum, siquidem quadrata fracta non excludantur,* tamen haec adiecta conditio maximum discrimen inter hanc demonstrationem et eam, quam desideramus, facit. Superest igitur demonstrandum, *qui numerus in fractis sit summa quatuor quadratorum, eundem quoque in integris quatuor quadratorum summae aequari.*

THEOREMA 1

1. *Ex serie quadratorum*

$$1,\ 4,\ 9,\ 16,\ 25\ etc.$$

nulli numeri per numerum primum p sunt divisibiles, nisi quorum radices sunt per eundem numerum p divisibiles.

DEMONSTRATIO

Si enim quispiam numerus quadratus aa fuerit per numerum primum p divisibilis, quia ex factoribus a et a constat, necesse est, ut alteruter factor per p sit divisibilis; quare numerus quadratus aa per numerum primum p divisibilis esse nequit, nisi eius radix a sit divisibilis per p.

COROLLARIUM 1

2. Numeri ergo quadrati per numerum primum p divisibiles nascuntur ex radicibus p, $2p$, $3p$, $4p$ etc. suntque ergo pp, $4pp$, $9pp$, $16pp$ etc. et reliqui numeri quadrati omnes per numerum primum p non erunt divisibiles.

COROLLARIUM 2

3. Si ergo numeri quadrati, quorum radices in hac progressione arithmetica p, $2p$, $3p$, $4p$ etc. non continentur, per numerum primum p dividantur, in divisione semper residuum remanebit, quod erit minus quam numerus p.

SCHOLION

4. Cuiusmodi sint haec residua, quae ex divisione singulorum quadratorum per numerum primum quemcunque p nascuntur, in hac dissertatione

1) Secundum manuscriptum; editio princeps: *temporum iactura.* F. R.

diligentius investigare constitui. Plurima enim hic insignia phaenomena occurrent, quorum consideratione natura numerorum non mediocriter illustratur. Tam eximia autem in doctrina numerorum adhuc latent mysteria, in quibus evolvendis opera non frustra impendi videtur.

THEOREMA 2

5. *Si series quadratorum in infinitum continuata in membra dispescatur, quorum singula ex p terminis constent, hoc modo*

$$1, 4, \ldots pp \mid (p+1)^2, \ldots 4pp \mid (2p+1)^2, \ldots 9pp \mid (3p+1)^2, \ldots 16pp \mid etc.,$$

tum si uniuscuiusque membri termini singuli per numerum primum p dividantur, eadem residua eodemque ordine recurrent.

DEMONSTRATIO

Singulorum enim membrorum termini primi $1, (p+1)^2, (2p+1)^2, (3p+1)^2$ etc. si per p dividantur, idem dabunt residuum $= 1$. Similique modo termini secundi $4, (p+2)^2, (2p+2)^2, (3p+2)^2$ etc. per p divisi aequalia producent residua $= 4$, siquidem sit $p > 4$. Eodemque modo patet terminos tertios aequalia praebere residua itemque quartos et quintos etc. Atque in genere si primi membri terminus quotuscunque sit nn, reliquorum membrorum termini analogi erunt $(p+n)^2, (2p+n)^2, (3p+n)^2$ etc., qui omnes per p divisi idem relinquunt residuum, quod terminus nn. In singulis ergo membris eadem redeunt residua eodemque ordine.

COROLLARIUM 1

6. Si igitur noverimus residua, quae ex terminis primi membri nascuntur, simul habebimus residua, quae ex divisione omnium reliquorum membrorum per numerum p facta oriuntur.

COROLLARIUM 2

7. Quia postremus cuiusque membri terminus per numerum p divisibilis existit, residuum erit $= 0$, quemadmodum primi cuiusque membri termini

residuum est $=1$. Secundorum vero terminorum cuiusque membri residuum erit $=4$ et tertiorum $=9$, quartorum $=16$ etc., siquidem sit $p>4$ et $p>9$ et $p>16$ etc.

COROLLARIUM 3

8. Quamdiu enim numeri quadrati 1, 4, 9, 16 etc. minores sunt quam numerus p, illi ipsi residua constituent. Ex sequentibus vero quadratis numero p maioribus residua emergent alia ipso numero p minora.

SCHOLION

9. Ex divisionis natura constat residua semper esse minora divisore p, ac si forte per inadvertentiam residuum relinquatur maius quam divisor p, id subtrahendo p, quoties fieri potest, ad numerum ipso p minorem reducetur. Sic residuum $p+a$ et in genere $np+a$, quod forte ex divisione per p prodierit, aequivalebit residuo a; atque cum de residuis, quae ex divisione numerorum per p nascuntur, agitur, omnia haec residua a, $p+a$, $2p+a$ et $np+a$ pro aequivalentibus haberi possunt, omnia scilicet redeunt ad minimum a; quae reductio cum sit in promtu, eam tuto negligere poterimus vel tanquam iam factam assumere. Ita si numeri quadrati 1, 4, 9, 16, 25 etc. per numerum p dividantur, nihil obstabit, quominus dicamus residua inde oriunda esse 1, 4, 9, 16, 25 etc., etiamsi hic numeri occurrant ipso divisore p maiores. De cetero notandum est hoc theorema vim suam retinere, sive divisor p sit numerus primus sive secus.

COROLLARIUM 4

10. Cum terminus ultimus pp primi membri nullum praebeat residuum, omnia residua, quae quidem ex tota serie quadratorum oriri possunt, nascentur ex his terminis 1, 4, 9, 16, ... $(p-1)^2$, quorum numerus est $=p-1$.

COROLLARIUM 5

11. Plura ergo diversa residua oriri nequeunt quam $p-1$; quod quidem per se est manifestum. Cum enim omnia residua sint ipso divisore p minora, omnium autem numerorum ipso p minorum numerus sit $=p-1$, etiam numerus residuorum diversorum numerus maior esse nequit.

THEOREMA 3

12. *Si omnes termini seriei quadratorum*

$$1, 4, 9, 16 \textit{ etc.}$$

per numerum quemcunque p dividantur ac residua notentur, inter haec residua non omnes numeri minores quam p occurrent.

DEMONSTRATIO

Omnia enim residua, quae quidem ex divisione omnium quadratorum per numerum p oriuntur, ex his terminis resultant

$$1, 4, 9, 16, \ldots (p-4)^2, (p-3)^2, (p-2)^2, (p-1)^2,$$

quorum terminorum numerus est $= p-1$; ideoque inde totidem residua proveniunt. Verum haec residua non omnia inter se sunt diversa; nam terminus ultimus $(p-1)^2 = pp - 2p + 1$ per p divisus residuum relinquit $= 1$, idem scilicet, quod primus terminus 1. Simili modo terminus penultimus $(p-2)^2 = pp - 4p + 4$ idem praebet residuum, quod terminus secundus 4; et terminus antepenultimus $(p-3)^2$ idem dat residuum, quod terminus tertius 9. Atque in genere terminus ordine n, qui est nn, idem dat residuum, quod terminus ordine $p-n$, qui est $(p-n)^2$. Cum igitur omnia residua, quae ex his terminis $1, 4, 9, \ldots (p-1)^2$ oriuntur et quorum numerus est $= p-1$, non sint inter se diversa, in iis non omnes numeri ipso p minores, quorum numerus est $= p-1$, occurrere possunt.

COROLLARIUM 1

13. Cum igitur bina residua semper sint aequalia, numerus diversorum residuorum ad semissem $\frac{p-1}{2}$ redigitur, siquidem sit $p-1$ numerus par; at si $p-1$ sit numerus impar seu p par, tum numerus diversorum residuorum erit $= \frac{p}{2}$; hoc enim casu dabitur residuum medium, quod sui aequale non habet.

COROLLARIUM 2

14. Cum igitur omnium numerorum ipso p minorum numerus sit $= p-1$, patet semissem horum numerorum in residuis locum habere; dabunturque ergo numeri, qui ex divisione numerorum quadratorum per numerum p nunquam relinquentur solo excepto casu, quo $p = 2$, quia $p - 1 = \frac{p}{2} = 1$.

COROLLARIUM 3

15. Quicunque ergo praeterea sit numerus p, per quem numeri quadrati dividantur, ex numeris ipso p minoribus semper erunt ad minimum $\frac{p-1}{2}$ vel $\frac{p-2}{2}$ numeri[1]), qui inter residua non reperiuntur. Prior casus valet, si p est numerus impar, posterior, si par.

COROLLARIUM 4

16. Hinc igitur numeri ipso divisore p minores, quorum multitudo est $= p-1$, sponte se in duas classes discriminant, quarum altera continet numeros in residuis locum habentes, altera vero eos, qui in classe residuorum non occurrunt. Hos numeros *non-residua* hic appellabo.

SCHOLION

17. Quo haec clarius percipiantur, iuvabit nonnulla exempla, in quibus residua et non-residua distinguuntur, inspexisse.

Sit	$p=3$	$p=4$	$p=5$	$p=6$
	1, 4	1, 4, 9	1, 4, 9, 16	1, 4, 9, 16, 25
residua	1, 1	1, 0, 1	1, 4, 4, 1	1, 4, 3, 4, 1
non-residua	2	2, 3	2, 3	2, 5

Sit	$p=7$	$p=8$
	1, 4, 9, 16, 25, 36	1, 4, 9, 16, 25, 36, 49
residua	1, 4, 2, 2, 4, 1	1, 4, 1, 0, 1, 4, 1
non-residua	3, 5, 6	2, 3, 5, 6, 7

Sit	$p=9$	$p=10$
	1, 4, 9, 16, 25, 36, 49, 64	1, 4, 9, 16, 25, 36, 49, 64, 81
residua	1, 4, 0, 7, 7, 0, 4, 1	1, 4, 9, 6, 5, 6, 9, 4, 1
non-residua	2, 3, 5, 6, 8	2, 3, 7, 8

1) Editio princeps (atque etiam *Comment. arithm.*): *vel* $\frac{p}{2}$ *numeri.* Correxit F. R.

Sit	$p = 11$
	1, 4, 9, 16, 25, 36, 49, 64, 81, 100
residua	1, 4, 9, 5, 3, 3, 5, 9, 4, 1
non-residua	2, 6, 7, 8, 10

Sit	$p = 12$
	1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121
residua	1, 4, 9, 4, 1, 0, 1, 4, 9, 4, 1
non-residua	2, 3, 5, 6, 7, 8, 10, 11.

Hinc perspicitur numerum non-residuorum interdum esse vel $\frac{p-1}{2}$ vel $\frac{p-2}{2}$, prout p fuerit numerus vel impar vel par, interdum esse etiam maiorem, nunquam vero esse minorem, omnino uti demonstratio theorematis postulat.[1])

THEOREMA 4

18. *Ut omnia residua, quae ex divisione quadratorum per numerum quemcunque p resultare possunt, inveniantur, tantum opus est quadrata ab unitate usque ad terminum $\left(\frac{p-1}{2}\right)^2$ vel $\left(\frac{p}{2}\right)^2$, prout p fuerit vel numerus impar vel par, per p dividere.*

DEMONSTRATIO

Ante iam demonstravimus omnia residua provenire ex divisione horum terminorum

$$1, \quad 4, \quad 9, \quad 16, \ldots (p-1)^2,$$

deinde vero vidimus seriem residuorum hinc natorum esse reciprocam seu ordine retrogrado scriptam eandem manere. Quare residua omnia, quatenus inter se sunt diversa, reperientur, si huius seriei termini tantum ad medietatem usque capiantur, unde, si p sit numerus impar ideoque $p-1$ par, omnes numeri, qui inter residua occurrunt, prodibunt ex his terminis

$$1, \quad 4, \quad 9, \quad 16, \ldots \left(\frac{p-1}{2}\right)^2.$$

1) Sed vide notam p. 343. F. R.

Sin autem p sit numerus par, quia superior progressio habet terminum medium, qui retrogrediendo sibi ipse respondet, residua omnia ex his terminis orientur

$$1, \quad 4, \quad 9, \quad 16, \ldots \left(\frac{p}{2}\right)^2.$$

COROLLARIUM 1

19. Si igitur p sit numerus impar, puta $p = 2q + 1$, omnia residua ex his tantum quadratis 1, 4, 9, 16, ... qq cognoscentur. At si p sit numerus par, puta $p = 2q$, haec quadrata 1, 4, 9, 16, ... qq omnia producent residua.

COROLLARIUM 2

20. Si haec residua omnia inter se fuerint inaequalia, cum eorum numerus sit $= q$, casu priori, quo $p = 2q + 1$ et $p - 1 = 2q$, numerus non-residuorum erit $= q$. Casu posteriori, quo $p = 2q$ et $p - 1 = 2q - 1$, omnium non-residuorum numerus erit $= q - 1$.

COROLLARIUM 3

21. Si a sit numerus quicunque non maior quam $\frac{p-1}{2}$ vel $\frac{p}{2}$ atque residuum constet, quod ex divisione quadrati aa per numerum p resultat, omnia quadrata in hac forma generali $(np \pm a)^2$ contenta idem praebebunt residuum. At numeri omnes omnino in forma $np \pm a$ includuntur, ita ut a non excedat vel $\frac{p-1}{2}$ vel $\frac{p}{2}$.

SCHOLION

22. Quo indolem numerorum, qui sunt residua, facilius explorare liceat, seriem residuorum repraesentemus his litteris 1, α, β, γ, δ, ε, ζ etc. pro divisore p, ita ut numerus horum terminorum sit vel $\frac{p-1}{2}$ vel $\frac{p}{2}$, prout p sit vel numerus impar vel par. Primo igitur patet in hac serie 1, α, β, γ, δ, ε etc. occurrere ordine omnes numeros quadratos 1, 4, 9, 16 etc., qui quidem sint ipso numero p minores, reliquos autem esse residua, quae in divisione maiorum quadratorum per eundem numerum p relinquuntur. Reliquas proprietates residuorum in sequentibus theorematis indagabimus.

THEOREMA 5

23. *Si in serie residuorum* 1, α, β, γ, δ *etc. occurrat numerus quicunque* r, *ibidem quoque reperientur omnes potestates ipsius* r^2, r^3, r^4, r^5 *etc. seu residua, quae ex harum potestatum divisione per numerum propositum* p *nascuntur.*

DEMONSTRATIO

Emergat residuum r ex quadrato aa, ita ut sit $aa = mp + r$; et quadratum $a^4 = (mp + r)^2$ per p divisum idem dabit residuum, quod oritur ex rr; atque ex quadrato $a^6 = (mp + r)^3$ idem oritur residuum, quod ex r^3; similique modo residua quadratorum a^8, a^{10}, a^{12} etc. convenient cum residuis terminorum r^4, r^5, r^6 etc. At residua ex omnibus quadratis quantumvis magnis oriunda iam proveniunt ex quadratis minimis 1, 4, 9, 16, ... $\left(\frac{p-1}{2}\right)^2$ vel $\left(\frac{p}{2}\right)^2$ ideoque continentur in serie residuorum 1, α, β, γ, δ etc. Ergo si in hac serie occurrit numerus r, ibidem quoque occurrent termini r^2, r^3, r^4, r^5 etc. seu residua, quae ex eorum divisione per divisorem propositum p relinquuntur.

COROLLARIUM 1

24. Quae igitur potestatum r^2, r^3, r^4, r^5 etc. fuerint minores quam p, eae ipsae in serie residuorum 1, α, β, γ, δ etc. reperientur. At altiores potestates sua residua, quae divisae per p relinquunt, ibidem introducent.

COROLLARIUM 2

25. Si sit $r = 1$, quia omnes eius potestates sunt $= 1$, ex iis nonnisi unicus terminus 1 in serie residuorum 1, α, β, γ, δ etc. nascitur. Neque ergo ex hoc casu novus terminus in serie residuorum cognoscitur.

COROLLARIUM 3

26. Quia in serie residuorum plures termini non occurrunt quam vel $\frac{p-1}{2}$ vel $\frac{p}{2}$, plura quoque residua diversa ex potestatibus r^2, r^3, r^4, r^5 etc., etiamsi in infinitum continuentur, prodire non possunt. Unde infinitae harum potestatum per p divisae aequalia praebebunt residua.

COROLLARIUM 4

27. Praebeant ergo hae potestates r^m et r^n idem residuum atque earum differentia $r^m - r^n$ per numerum p erit divisibilis seu $r^n(r^{m-n} - 1)$. Unde si factor r^n sit ad p primus, quod evenit, si residuum r fuerit ad p primum, alter factor $r^{m-n} - 1$ per p erit divisibilis ideoque potestas r^{m-n} per p divisa unitatem relinquet.

COROLLARIUM 5

28. Dabitur ergo potestas r^λ, quae per p divisa unitatem relinquit, quae utique in serie residuorum continetur, siquidem r sit numerus ad p primus. Tum autem potestas $r^{\lambda+1}$ dabit residuum r, potestas $r^{\lambda+2}$ residuum r^2 et $r^{\lambda+3}$ residuum r^3 etc. sicque hae potestates altiores eadem residua reproducunt, quae potestates inferiores r, r^2, r^3 etc.

COROLLARIUM 6

29. Cum igitur plura residua diversa provenire nequeant quam vel $\frac{p-1}{2}$ vel $\frac{p}{2}$, patet dari numerum λ non maiorem quam $\frac{p-1}{2}$ vel $\frac{p}{2}$, ita ut potestas r^λ per p divisa unitatem relinquat.

SCHOLION

30. Hinc ergo intelligitur, quomodo fieri possit, ut, etiamsi potestates r^2, r^3, r^4, r^5 etc. in infinitum progrediantur, tamen ex iis residua numero finita oriantur, si per divisorem p dividantur. Demonstravi quidem in dissertatione superiori[1]), si r sit numerus ad p primus, dari semper eiusmodi potestatem r^λ, quae per p divisa unitatem relinquat, ita ut sit $\lambda < p$. Nunc autem videmus, si r iam in serie residuorum ex quadratis natorum contineatur, tum exponentem λ etiam minorem fieri quam $\frac{p}{2}$.[2])

1) Vide primo Commentationes 54 et 134 huius voluminis, ubi ex aliis quidem principiis theorema FERMATIANUM aeque huc pertinens (numerum $r^{p-1} - 1$ esse per p divisibilem) demonstratum est. Deinde vero vide praecipue Commentationem 262 huius voluminis, § 15, ubi prima demonstratio directa ipsius theorematis, quod hic uti „in dissertatione superiori" demonstratum laudatur, exposita est. Accuratiore harum dissertationum comparatione maxime verisimile fit EULERUM Commentationem 262 ante Commentationem 242 conscripsisse. F. R.

2) Id quod etiam in theoremate 11 Commentationis 134 huius voluminis demonstratum est. Cf. porro huius voluminis Commentationem 262, § 66. F. R.

THEOREMA 6

31. *Si in serie residuorum* 1, α, β, γ, δ *etc., quae ex divisione numerorum quadratorum per numerum* p *oriuntur, occurrant numeri* r *et* s, *ibidem quoque occurret horum numerorum productum* rs *vel residuum, quod ex eius divisione per numerum* p *enascitur.*

DEMONSTRATIO

Proveniat residuum r ex quadrato aa et residuum s ex quadrato bb; erit $aa = mp + r$ et $bb = np + s$; hinc fiet quadratum

$$aabb = mnpp + msp + nrp + rs,$$

quod ergo per p divisum residuum relinquet rs, vel si $rs > p$, idem relinquet residuum, quod oritur ex rs. Quare cum residuum ex quadrato $aabb$ natum in serie residuorum contineatur, ibi quoque rs seu residuum inde ortum reperietur.

COROLLARIUM 1

32. In serie ergo residuorum 1, α, β, γ, δ etc. si occurrant duo numeri r et s, ibidem quoque occurrent non solum potestates r, r^2, r^3, r^4 etc. et s, s^2, s^3, s^4 etc., sed etiam producta ex binis terminis quibuscunque rs, r^2s, rs^2, r^3s, r^2s^2, rs^3 etc.

COROLLARIUM 2

33. Hinc igitur patet, si formula $\frac{1}{(1-r)(1-s)}$ in seriem resolvatur

$$1 + r + s + rr + rs + ss + r^3 + rrs + rss + s^3 + \text{etc.},$$

singulos terminos huius seriei in serie residuorum occurrere vel etiam residua ex his terminis divisione per p orta.

COROLLARIUM 3

34. Etiamsi autem horum terminorum numerus sit infinitus, tamen constat plura ex iis residua diversa produci non posse quam vel $\frac{p-1}{2}$ vel $\frac{p}{2}$, prout p fuerit numerus vel impar vel par.

SCHOLION

35. Quo clarius appareat, quomodo ex his terminis numero infinitis tamen residuorum diversorum numerus finitus et quidem non maior quam $\frac{p-1}{2}$ vel $\frac{p}{2}$ oriatur, evolvamus exemplum aliquod sitque $p = 19$; erit $\frac{p-1}{2} = 9$, unde ex his quadratis

1, 4, 9, 16, 25, 36, 49, 64, 81

orientur residua

1, 4, 9, 16, 6, 17, 11, 7, 5.

Ex hac serie residuorum contemplemur hos duos numeros 5 et 6, ex quibus formemus primo series potestatum

5, 25, 125, 625, 3125, 15625, 78125 etc.,

6, 36, 216, 1296, 7776, 46656, 279936 etc.

Ex illa serie per $p = 19$ divisa prodeunt residua

5, 6, 11, 17, 9, 7, 16, 4, 1;

sequens scilicet residuum semper invenitur, si praecedens per 5 multiplicetur et productum, si sit > 19, infra 19 deprimatur. Simili modo ex potestatibus numeri 6 haec prodibunt residua

6, 17, 7, 4, 5, 11, 9, 16, 1.

Porro si haec singula residua per singula superiora multiplicentur et producta infra 19 deprimantur, iidem prodeunt numeri; multiplicetur enim inferior series primo per 5, tum per 6, 11, 17 etc., ut sequitur,

per 5:	11,	9,	16,	1,	6,	17,	7,	4,	5,
per 6:	17,	7,	4,	5,	11,	9,	16,	1,	6,
per 11:	9,	16,	1,	6,	17,	7,	4,	5,	11,
per 17:	7,	4,	5,	11,	9,	16,	1,	6,	17,
per 9:	16,	1,	6,	17,	7,	4,	5,	11,	9,
per 7:	4,	5,	11,	9,	16,	1,	6,	17,	7,
per 16:	1,	6,	17,	7,	4,	5,	11,	9,	16,
per 4:	5,	11,	9,	16,	1,	6,	17,	7,	4.

Perspicitur igitur, quomodocunque hi numeri 1, 4, 9, 16, 6, 17, 11, 7, 5 seriem residuorum constituentes inter se per multiplicationem combinentur, siquidem divisione per 19 facta infra 19 deprimantur, eosdem semper numeros recurrere neque unquam ullum numerum eorum, qui non sunt residua, nempe 2, 3, 8, 10, 12, 13, 14, 15, 18, prodire.

COROLLARIUM 4

36. Si ergo sit 1, α, β, γ, δ etc. series residuorum omnium, quae ex divisione quadratorum per numerum p resultant, in eadem serie quoque occurrent omnia producta ex binis pluribusve numerorum α, β, γ, δ etc. Ergo si haec expressio $\frac{1}{(1-\alpha)(1-\beta)(1-\gamma)(1-\delta)\text{ etc.}}$ in seriem evolvatur, omnes eius termini in serie residuorum occurrent.

THEOREMA 7

37. *Si in serie residuorum* 1, α, β, γ, δ *etc., quae ex divisione quadratorum per numerum p prodeunt, reperiantur numeri r et rs, qui sint ad p primi, quorum ille huius est factor, tunc in eadem residuorum serie etiam numerus s continebitur.*

DEMONSTRATIO

Proveniat residuum r ex quadrato aa et rs ex bb; erit $aa = mp + r$ et $bb = np + rs$; unde fit $bb - aas = np - mps$ sicque $bb - aas$ erit per p divisibile. At cum r et rs sint numeri ad p primi, erunt quoque quadrata aa et bb ad p prima; unde si haec quadrata aa et bb inter se non sint prima, per communem divisorem quadratum ad prima reduci poterunt, ita ut $bb - aas$ maneat per p divisibile. Sint ergo b et a numeri inter se primi[1]), atque cum etiam haec forma $(mp \pm b)^2 - aas$ sit per p divisibilis, semper pro m eiusmodi numerus assignari potest, ut fiat $mp \pm b$ multiplum ipsius a. Sit ergo $mp \pm b = ac$; erit $aacc - aas$ per p divisibile; quod cum sit $= aa(cc - s)$ alterque factor aa sit ad p primus, necesse est, ut alter factor

1) Ad hoc autem observandum est nihil plane interesse, utrum a et b inter se sint primi necne, atque ad aequationem $mp \pm b = ac$ constituendam prorsus sufficere numerum a ad p esse primum. F. R.

$cc - s$ per p sit divisibilis, unde quadratum cc per p divisum relinquet s, ex quo numerus s in serie residuorum $1, \alpha, \beta, \gamma, \delta$ etc. reperietur, siquidem ibi numeri r et rs occurrant iique sint ad p primi.

COROLLARIUM 1

38. Ut igitur veritas theorematis consistat, necesse est, ut numeri r et rs seu r et s sint ad divisorem p primi. Supra enim vidimus, si sit $p = 12$, in residuis reperiri numeros 4 et 0 seu 4 et 12; hinc autem posito $r = 4$ et $rs = 12$ non sequitur numerum $s = 3$ in residuis reperiri, quia r et s non sunt numeri ad p primi; ac revera etiam numerus 3 inter non-residua continetur.

COROLLARIUM 2

39. Sin autem divisor p sit numerus primus, quia tum omnia residua $\alpha, \beta, \gamma, \delta$ etc. ad eum sunt prima, si in iis occurrant numeri r et rs, tum etiam certo in iis occurret numerus s.

COROLLARIUM 3

40. Si inter residua occurrant numeri r et s primi ad p, quia residuo r aequivalentia censenda sunt residua $p + r$, $2p + r$ et in genere $np + r$, si fuerit $np + r = ts$, tum etiam numerus t inter residua reperietur.

SCHOLION

41. Ne ad huiusmodi exceptiones, quando residua non sunt numeri ad p primi, respicere obligemur, in sequentibus ponamus divisorem p semper esse numerum primum; et cum residua ex binario orta sint obvia, sit divisor p simul numerus impar seu $p = 2q + 1$; tum ergo series residuorum formabitur ex his terminis

$$1, \quad 4, \quad 9, \quad 16, \; \ldots \; qq,$$

ita ut eorum numerus, quatenus inter se sunt diversa, maior esse nequeat quam q. Si igitur residua ex hoc divisore primo $p = 2q + 1$ sint $1, \alpha, \beta, \gamma, \delta$ etc., in hac serie non solum producta ex binis pluribusve terminorum $\alpha, \beta, \gamma, \delta$ etc. occurrent, sed quia omnia haec residua ad p sunt prima, si inter ea occurrant r et rs, ita ut unum per aliud sit divisibile, tum etiam quotus inde natus s in eadem serie residuorum continebitur.

THEOREMA 8

42. *Si ex divisore primo $p = 2q + 1$, per quem omnes numeri quadrati dividantur, nascatur series residuorum 1, α, β, γ, δ, ε etc., quorum numerus est $= q$, omnia haec residua inter se erunt inaequalia.*

DEMONSTRATIO

Primo patet nullum residuum in hac serie esse posse $= 0$; cum enim nascantur ex quadratis ipso qq non maioribus, nullum horum quadratorum per numerum primum $p = 2q + 1$ est divisibile; igitur cyphra inter residua multo minus bis occurrere poterit. Ponamus autem duo residua, quae ex quadratis aa et bb oriuntur, esse aequalia eritque differentia horum quadratorum $aa - bb$ per divisorem $p = 2q + 1$ divisibilis. At cum omnia haec residua 1, α, β, γ, δ etc. ex quadratis minimis, quae qq non excedunt, oriantur, quadrata illa aa et bb non superabunt qq eritque propterea neque $a > q$ neque $b > q$ neque idcirco $a + b > 2q$, unde certo erit $a + b < p$. Cum igitur differentia quadratorum $aa - bb$ esset per p divisibilis, siquidem residua inde nata essent aequalia, et p sit numerus primus, vel summa $a + b$ vel differentia $a - b$ foret per p divisibilis; utrumque autem ob tam $a - b < p$ quam $a + b < p$ fieri nequit. Ergo omnia residua, quae ex divisione quadratorum 1, 4, 9, 16, ... qq per numerum primum $p = 2q + 1$ resultant, inter se sunt inaequalia.

COROLLARIUM 1

43. Numerus igitur omnium residuorum diversorum, quae ex divisione quadratorum per numerum primum $p = 2q + 1$ oriuntur, certo est $= q$; ante enim ostensum est eum non esse maiorem quam q, hic autem evicimus eum non esse minorem quam q.

COROLLARIUM 2

44. Cum numerus omnium numerorum ipso divisore $p = 2q + 1$ minorum sit $= p - 1 = 2q$, patet horum numerorum semissem tantum in serie residuorum 1, α, β, γ, δ etc. occurrere eamque constituere, alterum vero semissem constituere seriem non-residuorum ideoque, si p sit numerus primus, seriem non-residuorum etiam ex q numeris constare.

COROLLARIUM 3

45. Si ergo x sit numerus quicunque ex serie non-residuorum divisori p respondentium, certo affirmare possumus, quicquid sit n, nullum numerum in hac forma $np + x$ esse posse quadratum.

SCHOLION

46. Quia nunc investigationes nostras tantum ad divisores primos dirigimus, expediet tam residua quam non-residua, quae minoribus numeris primis respondent, hic exhibere. In genere scilicet, si divisor sit p, seriem residuorum per $1, \alpha, \beta, \gamma, \delta$ etc. et seriem non-residuorum per a, b, c, d, e etc. repraesentamus; et quo facilius coniunctim tam residua quam non-residua referantur, hoc modo exponemus:

$$p\begin{Bmatrix} 1, & \alpha, & \beta, & \gamma, & \delta, & \varepsilon, & \zeta & \text{etc.} \\ a, & b, & c, & d, & e, & f, & g & \text{etc.} \end{Bmatrix}$$

Duas nimirum series numerorum quovis casu scribemus, quarum superior residua, inferior non-residua continet, et utrique divisorem p, ad quem pertinent, praefigemus. Hoc modo residua et non-residua, quae ex divisoribus primis simplicioribus resultant, ita indicabuntur:

$$3\begin{Bmatrix} 1 \\ 2 \end{Bmatrix}, \quad 5\begin{Bmatrix} 1, & 4 \\ 2, & 3 \end{Bmatrix}, \quad 7\begin{Bmatrix} 1, & 4, & 2 \\ 3, & 5, & 6 \end{Bmatrix}, \quad 11\begin{Bmatrix} 1, & 4, & 9, & 5, & 3 \\ 2, & 6, & 7, & 8, & 10 \end{Bmatrix},$$

$$13\begin{Bmatrix} 1, & 4, & 9, & 3, & 12, & 10 \\ 2, & 5, & 6, & 7, & 8, & 11 \end{Bmatrix}, \quad 17\begin{Bmatrix} 1, & 4, & 9, & 16, & 8, & 2, & 15, & 13 \\ 3, & 5, & 6, & 7, & 10, & 11, & 12, & 14 \end{Bmatrix},$$

$$19\begin{Bmatrix} 1, & 4, & 9, & 16, & 6, & 17, & 11, & 7, & 5 \\ 2, & 3, & 8, & 10, & 12, & 13, & 14, & 15, & 18 \end{Bmatrix}, \quad 23\begin{Bmatrix} 1, & 4, & 9, & 16, & 2, & 13, & 3, & 18, & 12, & 8, & 6 \\ 5, & 7, & 10, & 11, & 14, & 15, & 17, & 19, & 20, & 21, & 22 \end{Bmatrix},$$

$$29\begin{Bmatrix} 1, & 4, & 9, & 16, & 25, & 7, & 20, & 6, & 23, & 13, & 5, & 28, & 24, & 22 \\ 2, & 3, & 8, & 10, & 11, & 12, & 14, & 15, & 17, & 18, & 19, & 21, & 26, & 27 \end{Bmatrix}.$$

Residua hic eo ordine, quo ex quadratis nascuntur, sunt posita, non-residua autem, quia nullo ordine connectuntur, a minimis ad maiora progrediendo collocavimus. Exempla haec quoque in eum finem servire poterunt, ut in iis proprietates residuorum ante demonstratae examinentur.

THEOREMA 9

47. *Si ex divisione quadratorum per numerum primum $p = 2q + 1$ nascatur haec series residuorum* $1, \alpha, \beta, \gamma, \delta$ *etc. haecque series non-residuorum* a, b, c, d, e *etc. atque in hac serie non-residuorum occurrat numerus* r, *in eadem quoque occurrent omnes hi numeri* $\alpha r, \beta r, \gamma r, \delta r$ *etc. vel eorum residua divisione per* p *relicta.*

DEMONSTRATIO

Quicunque enim horum numerorum, ut αr, vel in serie residuorum continetur vel in serie non-residuorum. At cum α in serie residuorum contineatur, si αr ibidem contineretur, necessario quoque r in serie residuorum existeret. Quare, cum per hypothesin r sit numerus ex serie non-residuorum, numerus αr non erit in serie residuorum; habebit ergo αr locum in serie non-residuorum, quod idem de numeris $\beta r, \gamma r, \delta r$ etc. valet. Quod autem demonstravimus de his productis $\beta r, \gamma r, \delta r$ etc., si sint maiora quam p, id intelligendum est de residuis, quae haec producta per p divisa relinquunt.

COROLLARIUM 1

48. Quia omnes numeri $1, \alpha, \beta, \gamma, \delta$ etc., quorum numerus est $= q$, sunt inter se diversi, sequitur quoque omnes hos numeros $r, \alpha r, \beta r, \gamma r, \delta r$ etc. esse inter se diversos; unde, si omnia residua habeantur, ex unico non-residuo cognito reliqua omnia non-residua definiuntur.

COROLLARIUM 2

49. Dabit ergo series $r, \alpha r, \beta r, \gamma r, \delta r$ etc. omnia plane non-residua; continet enim q numeros diversos totidemque et non plura existunt non-residua, siquidem divisor p est numerus primus.

COROLLARIUM 3

50. Si ergo ex serie non-residuorum quilibet alius numerus s capiatur, eius producta $\alpha s, \beta s, \gamma s$ etc. alios numeros pro non-residuis[1]) non praebent, nisi qui ex quovis alio r hoc modo sunt reperti.

1) Editio princeps (atque etiam *Comment. arithm.*): *pro residuis.* Correxit F. R.

THEOREMA 10

51. *Producta ex binis numeris seriei non-residuorum continentur in serie residuorum, siquidem haec residua nascantur ex divisione numerorum quadratorum per quempiam numerum primum.*

DEMONSTRATIO

Sit enim $p = 2q + 1$ divisor primus atque series residuorum sit 1, α, β, γ, δ etc., series autem non-residuorum sit a, b, c, d, e etc. Vidimus autem, si r sit non-residuum quodcunque, seriem non-residuorum hoc modo quoque exhiberi

$$r, \quad \alpha r, \quad \beta r, \quad \gamma r, \quad \delta r \quad \text{etc.}$$

Iam productum ex duobus quibuscunque horum terminorum $\alpha\beta r^2$ constat ex duobus factoribus $\alpha\beta$ et rr, quorum uterque in serie residuorum continetur, quia omnia quadrata ac propterea etiam rr ibi occurrunt; unde perspicuum est productum ex binis quibusque non-residuis in serie residuorum contineri.

COROLLARIUM 1

52. Ut igitur productum ex duobus residuis dat residuum, ita quoque productum ex duobus non-residuis dabit residuum. Sed productum ex residuo et non-residuo semper producit non-residuum.

COROLLARIUM 2

53. Hinc etiam sequitur, uti residuum per residuum divisum dat residuum, ita quoque non-residuum per non-residuum divisum dare residuum. Verum residuum per non-residuum vel vicissim non-residuum per residuum divisum praebet non-residuum.

COROLLARIUM 3

54. Quemadmodum bina non-residua invicem multiplicata residuum producunt, ita terna non-residua invicem multiplicata praebebunt non-residuum; quaterna vero non-residua iterum residuum producunt, at quina non-residuum, et sic deinceps.

DEFINITIO

55. *Complementum residui est eius defectus a divisore, ex quo est ortum; sic si divisor sit* $= p$ *et residuum* $= r$, *erit complementum residui* $= p - r$.

COROLLARIUM 1

56. Quia ratione residuorum omnes hi numeri r, $p + r$, $2p + r$ et in genere $np + r$ pro iisdem habentur, quicunque numerus pro n sumatur, erit eorum complementum $= p - np - r$; unde si sumatur $n = 1$, complementum residui r erit $= -r$.

COROLLARIUM 2

57. Si n sumatur $= -1$, residuum r etiam per $r - p$ exprimi potest, ita ut sit negativum. In divisione enim si quotus nimis magnus accipitur, ad residua negativa pervenitur. Sic residuum affirmativum r aequivalebit residuo negativo $r - p$.

COROLLARIUM 3

58. Si sit $r > \frac{1}{2}p$, tum hoc residuum negative exprimi poterit per $r - p$, quod erit minus quam $\frac{1}{2}p$. Ita si expressiones negativae in usum vocentur, omnia residua per numeros exhiberi poterunt semisse divisoris $\frac{1}{2}p$ non maiores. Sic pro divisore $p = 23$ habebuntur haec residua per numeros non maiores quam $\frac{23}{2}$ expressa

$$1, \quad 4, \quad 9, \quad -7, \quad 2, \quad -10, \quad 3, \quad -5, \quad -11, \quad 8, \quad 6.$$

COROLLARIUM 4

59. Similique modo non-residua etiam per numeros ipso $\frac{1}{2}p$ non maiores exhiberi poterunt eruntque pro divisore $p = 23$ haec non-residua

$$5, \quad 7, \quad 10, \quad 11, \quad -9, \quad -8, \quad -6, \quad -4, \quad -3, \quad -2, \quad -1.$$

Unde si $p = 2q + 1$, numerus tam residuorum quam non-residuorum erit $= q$ neque in utraque serie occurrunt numeri maiores quam q.

COROLLARIUM 5

60. Si hoc modo residua exprimantur, statim patet, utrum cuiuspiam residui complementum in eadem serie residuorum contineatur necne. Nempe si r sit residuum, erit $-r$ eius complementum, et vicissim si $-r$ sit residuum, erit $+r$ eius complementum. Quare nisi in serie residuorum idem numerus bis occurrat, affirmative scilicet et negative, eius complementum in serie residuorum non continetur.

THEOREMA 11

61. *Si in serie residuorum* $1, \alpha, \beta, \gamma, \delta$ *etc., quae ex divisione quadratorum per numerum primum* $p = 2q + 1$ *generantur, unius termini occurrat complementum, tum simul omnium terminorum complementa in eadem serie occurrent.*

DEMONSTRATIO

Sit r id residuum, cuius complementum $-r$ quoque in serie $1, \alpha, \beta, \gamma, \delta$ etc. occurrat. Cum igitur $-r$ per r divisum det -1, in eadem serie quoque numerus -1 occurret seu valor cuiuspiam litterarum $\alpha, \beta, \gamma, \delta$ etc. erit $= -1$. Quoniam ergo in eadem serie producta ex binis terminis simul reperiuntur, ibidem occurrent termini $-\alpha, -\beta, -\gamma, -\delta$ etc. Cuiusvis ergo residui complementum simul in serie residuorum reperietur, siquidem unici termini complementum in ea occurrat.

COROLLARIUM 1

62. Si ergo unici termini r complementum $-r$ in serie residuorum contineatur, tum quilibet numerus huius seriei bis occurret, primo scilicet affirmative, tum vero etiam negative. In serie nempe residuorum $1, \alpha, \beta, \gamma, \delta$ etc. etiam continebuntur termini $-1, -\alpha, -\beta, -\gamma, -\delta$ etc.

COROLLARIUM 2

63. Cum igitur hoc casu in serie residuorum quilibet terminus bis occurrat, numerus omnium terminorum necessario erit par. At numerus omnium terminorum est $= q$; ergo nisi sit q numerus par, fieri nequit, ut complementa residuorum simul in serie residuorum contineantur.

COROLLARIUM 3

64. Si igitur q est numerus impar, puta $q = 2n + 1$, ita ut sit $p = 4n + 3$, in serie residuorum nullus plane occurrit numerus, cuius complementum simul in ea serie contineatur. Omnia ergo complementa hoc casu in seriem non-residuorum ingredientur eritque utrinque terminorum numerus impar $= q = 2n + 1$.

SCHOLION

65. Hinc ergo summum discrimen agnoscitur, quod inter numeros primos $p = 2q + 1$ intercedit, prout q fuerit numerus par vel impar, cum posteriori casu certo sciamus nullius residui complementum in residuorum serie contineri. Quodsi ergo priori casu ponamus $q = 2n$, posteriori $q = 2n - 1$, illo casu erit numerus primus $p = 4n + 1$, hoc vero $p = 4n - 1$; unde patet omnes numeros primos binario excepto vel unitate superare multiplum quaternarii vel unitate ab eo deficere sicque duas obtinemus numerorum classes, quarum altera in forma $4n + 1$, altera in forma $4n - 1$ continetur. Prioris classis $4n + 1$ sunt ergo numeri primi 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97 etc., posterioris vero classis $4n - 1$ hi 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83 etc. De numeris primis classis prioris FERMATIUS olim pronunciavit singulos esse aggregata duorum quadratorum[1]), cuius theorematis veritatem nuper tandem post plures conatus demonstravi.[2]) De numeris autem posterioris classis facile ostenditur nullum eorum esse summam duorum quadratorum; quin etiam mox demonstrabo ne quidem summam duorum quadratorum $aa + bb$ exhiberi posse, quae sit per eiusmodi numerum primum $p = 4n - 1$ divisibilis, nisi utrumque quadratum aa et bb seorsim per eum divisibile existat.[3]) De his tamen numeris FERMATIUS affirmavit singulos vel esse trium vel quatuor quadratorum aggregata[4]); ita videmus esse $3 = 1 + 1 + 1$,

1) Vide notam 2 p. 310. F. R.

2) Vide Commentationes 228 et 241 huius voluminis. F. R.

3) Hoc theorema alia quidem methodo EULERUS iam in Commentatione 134, § 16, huius voluminis demonstravit, ubi addere liceat EULERUM illam demonstrationem iam epistola d. 6. Martii 1742 scripta cum CHR. GOLDBACH communicavisse. Vide *Correspondance math. et phys. publiée par P. H. Fuss*, St.-Pétersbourg 1843, t. I, p. 114; *LEONHARDI EULERI Opera omnia*, series III. F. R.

4) Integra FERMATII affirmatio haec est: „*Imo propositionem pulcherrimam et maxime generalem nos primi deteximus: nempe omnem numerum vel esse triangulum vel ex duobus aut tribus*

$7 = 1 + 1 + 1 + 4$, $11 = 1 + 1 + 9$, $19 = 1 + 9 + 9$, $23 = 1 + 4 + 9 + 9$, $31 = 4 + 9 + 9 + 9 = 1 + 1 + 4 + 25$ etc., verum nullum existere huiusmodi numerum, qui non ad minimum in quatuor quadrata resolvi possit. Etsi FERMATIUS eius demonstrationem se invenisse sit professus, tamen nusquam eam publicavit, ita ut cum ipso penitus interiisse videatur, neque deinceps quisquam inventus est, qui hanc demonstrationem, quae in analysi DIOPHANTEA et universa numerorum scientia maximi est momenti, reperire potuerit. Equidem hic demonstrabo quocunque proposito numero primo $4n - 1$ semper summam quatuor quadratorum, quin etiam trium, exhiberi posse, quae per eum sit divisibilis. Cum igitur etiam demonstrari queat productum ex duobus numeris, quorum uterque est summa [quatuor] quadratorum, etiam esse quatuor quadratorum aggregatum, non procul a demonstratione desiderata abesse videmur. Tantum enim superest, ut demonstretur, si summa quatuor quadratorum fuerit divisibilis per numerum, qui etiam sit summa quatuor quadratorum, quotum quoque certo fore summam quatuor quadratorum.

THEOREMA 12

66. *Si omnia quadrata per numerum primum* $= 4n - 1$ *dividantur indeque oriatur series residuorum* $1, \alpha, \beta, \gamma, \delta$ *etc., nullius residui complementum simul in hac serie residuorum continebitur.*

---

triangulis compositum; esse quadratum vel ex duobus aut tribus aut quatuor quadratis compositum; esse pentagonum vel ex duobus, tribus, quatuor aut quinque pentagonis compositum; et sic deinceps in infinitum, in hexagonis, heptagonis et polygonis quibuslibet, enuntianda videlicet pro numero angulorum generali et mirabili propositione." Vide FERMATII observationes ad BACHETI commentarium in quaestionem XXXI libri IV DIOPHANTI *Arithmeticorum* (cf. notam 2 p. 51 huius voluminis); *Oeuvres de FERMAT*, t. I, p. 305. Vide etiam FERMATII epistolas ad KENELMUM DIGBY (1658) et CARCAVI (1659) scriptas, quae nota 2 p. 310 laudatae sunt.

Observandum quidem est iam DIOPHANTUM in nonnullis libri quarti et quinti quaestionibus omnem numerum in quatuor quadrata dividi posse tacite supposuisse. Theorema autem „*omnem numerum vel quadratum esse, vel ex duobus, aut tribus, aut etiam quatuor quadratis componi*" hac forma primum a BACHETO enuntiatum est; vide BACHETI commentarium supra commemoratum in celebri editione, quae inscribitur *DIOPHANTI Alexandrini Arithmeticorum libri sex et de numeris multangulis liber unus.* Nunc primum graece et latine editi, atque absolutissimis commentariis illustrati. Auctore C. G. BACHETO, Lutetiae Parisiorum 1621. BACHETUS ibi (p. 241) ingenue confitetur perfecta quidem demonstratione illud theorema assequi se non potuisse, interim tamen id inductione confirmasse ostendendo proprium esse numerorum omnium ab 1 usque ad 120. Quibus compositionibus communicatis affirmat „de omnibus numeris usque ad 325 experimentum se sumpsisse". F. R.

DEMONSTRATIO

Omnia residua

$$1, \alpha, \beta, \gamma, \delta, \ldots \nu$$

resultant ex divisione horum quadratorum

$$1, 4, 9, 16, 25, \ldots (2n-1)^2;$$

numerus ergo horum residuorum est $= 2n - 1$ ideoque impar. At si unius residui α complementum $p - \alpha$ seu $-\alpha$ in eadem serie extaret, tum simul omnium residuorum complementa ibidem occurrere deberent sicque, cum unumquodque residuum bis, nempe cum signo $+$ et cum signo $-$ adesset, numerus residuorum esset par. Quare cum sit impar, fieri nequit, ut vel unici residui complementum simul in eadem residuorum serie contineatur.

COROLLARIUM 1

67. Si ultimus seriei residuorum terminus ponatur $= \nu$, quia oritur ex quadrato $(2n-1)^2 = 4nn - 4n + 1$ per $4n - 1$ diviso, erit residuum $\nu = -3n + 1$ seu $= n$ sumto quoto $n - 1$. Ergo eius complementum $-n$ seu $3n - 1$ in serie residuorum non reperitur. Numerus ergo $-n$ seu $3n - 1$ certo erit in serie non-residuorum.

COROLLARIUM 2

68. Cum $mp - n$ seu $m(4n-1) - n$ omnes numeros complectatur, qui per $4n - 1$ divisi residuum dant $-n$, patet nullum horum numerorum $m(4n-1) - n$ seu $4mn - m - n$ unquam esse posse quadratum.[1])

1) Hoc theorema, quod etiam invenitur in huius voluminis Commentatione 164, EULERUS in epistola d. 9. Sept. 1741 ad CHR. GOLDBACH scripta his verbis proposuit: „Ich habe vor langer Zeit auch solche ähnliche theoremata gefunden, als $4mn - m - 1$ kann nullo modo ein Quadrat seyn. Item $4mn - m - n$ kann auch kein Quadrat seyn, positis m et n numeris integris affirmativis." Vide *Correspondance math. et phys. publiée par P. H. Fuss*, St.-Pétersbourg 1843, t. I, p. 105 (vide ibidem sequentes quoque epistolas ab EULERO ad CHR. GOLDBACH et ab hoc ad EULERUM usque ad a. 1744 scriptas); *LEONHARDI EULERI Opera omnia*, series III. F. R.

COROLLARIUM 3

69. Cum in serie residuorum occurrant numeri quadrati 1, 4, 9, 16 etc., in eadem certe non occurrent eorum complementa -1, -4, -9, -16 etc. Numeri ergo quadrati signo $-$ affecti in seriem non-residuorum ingredientur.

THEOREMA 13

70. *Non datur summa duorum quadratorum, quae sit divisibilis per numerum primum formae $4n-1$, nisi utrumque quadratum seorsim per eundem sit divisibile, seu non datur summa duorum quadratorum inter se primorum per numerum primum $4n-1$ divisibilis.*

DEMONSTRATIO

Ponamus enim summam duorum quadratorum $aa+bb$ esse per numerum primum $4n-1$ divisibilem neque tamen vel aa vel bb seorsim esse per $4n-1$ divisibile. Sit ergo r residuum, quod in divisione quadrati aa per $4n-1$ relinquitur, et s residuum ex divisione quadrati bb ortum; atque tam r quam s in serie residuorum 1, α, β, γ, δ etc. occurret. Iam summa quadratorum $aa+bb$ per $4n-1$ divisa relinquet residuum $r+s$; quod cum per hypothesin esse debeat $=$ divisori $4n-1$, erit $s=4n-1-r$ seu $s=-r$ ideoque s erit complementum residui r. Quare si r in serie residuorum contineatur, eius complementum s in ea certe non occurret; unde sumto quadrato quocunque aa nullum datur aliud quadratum bb eiusmodi, ut summa $aa+bb$ fiat per numerum primum $4n-1$ divisibilis, nisi ipsum quadratum aa per se sit divisibile per $4n-1$, quo casu etiam bb per $4n-1$ divisibile esse debet. Nulla ergo datur summa duorum quadratorum inter se primorum, quae sit per numerum primum $4n-1$ divisibilis.[1])

COROLLARIUM 1

71. Non ergo datur huiusmodi formae $aa+1$ numerus, qui sit per numerum primum $4n-1$ divisibilis. Ad hoc enim opus esset, ut residuum ex quadrato aa ortum esset $=-1$, quod autem in serie residuorum non existit.

1) Vide notam 3 p. 358. F. R.

COROLLARIUM 2

72. Cum summa duorum quadratorum $aa+bb$ per nullum numerum primum formae $4n-1$ sit divisibilis, etiam per nullum numerum compositum p, qui factorem primum habet formae $4n-1$, erit divisibilis; si enim per hunc numerum p esset divisibilis, etiam per eius factorem $4n-1$ divisibilis foret.

THEOREMA 14

73. *Sive numerus* $4n-1$ *sit primus sive compositus, nulla datur summa duorum quadratorum inter se primorum per eum numerum* $4n-1$ *divisibilis.*

DEMONSTRATIO

Si enim numerus $4n-1$ sit primus, iam demonstrata est veritas theorematis. At si $4n-1$ non sit numerus primus, erit productum ex aliquot numeris primis et quidem imparibus, cum ipse numerus $4n-1$ sit impar. Omnes autem numeri primi sunt vel formae $4m+1$ vel $4m-1$; sed omnes factores numeri $4n-1$ esse nequeunt formae $4m+1$; quotcunque enim numeri huius formae $4m+1$ in se invicem multiplicentur, productum semper erit numerus formae $4n+1$ seu unitate excedet multiplum quaternarii. Quare necesse est, ut numerus $4n-1$ unum ad minimum habeat factorem primum formae $4m-1$, et quia per talem numerum primum nulla summa duorum quadratorum inter se primorum est divisibilis, nulla etiam datur, quae per numerum compositum $4n-1$ esset divisibilis.

COROLLARIUM 1

74. Cum nulla detur summa duorum quadratorum inter se primorum per numerum $4n-1$, sive sit primus sive compositus, divisibilis, multo minus numerus $4n-1$ ipse erit summa duorum quadratorum. Si enim esset $4n-1=aa+bb$, utrumque quadratum aa et bb seorsim per $4n-1$ divisibile esse deberet, quod, cum utrumque sit minus quam $4n-1$, fieri nequit.

SCHOLION

75. Nullum numerum formae $4n-1$ esse posse summam duorum quadratorum etiam facillime hoc modo ostenditur. Si enim numerus $4n-1$

esset summa duorum quadratorum, alterum esse deberet par, alterum impar. At omnia quadrata paria sunt numeri huius formae $4f$ et omnia quadrata imparia numeri huius formae $4g+1$. Summa ergo duorum quadratorum, quorum alterum est par, alterum impar, erit numerus formae $4f+4g+1$ seu $4n+1$; ergo numerus formae $4n-1$ non potest esse summa duorum quadratorum.[1])

COROLLARIUM 2

76. Nullus etiam numerus, qui factorem habet formae $4n-1$, potest esse divisor summae duorum quadratorum inter se primorum; si enim esset divisor, etiam eius factor $4n-1$ foret divisor, quod fieri nequit.

COROLLARIUM 3

77. Multo ergo minus huiusmodi numerus, qui factorem habet $4n-1$, esse potest summa duorum quadratorum inter se primorum. Ita impossibile est, ut sit $m(4n-1)=aa+bb$, siquidem a et b sint numeri inter se primi.

THEOREMA 15

78. *Nullus numerus in hac forma $4mn-m-n$ contentus, quicunque numeri pro m et n capiantur, unquam esse potest quadratum.*[2])

DEMONSTRATIO

Cum nullus numerus, qui factorem habet $4n-1$, esse queat summa duorum quadratorum inter se primorum, seu quae praeter unitatem nullum habeant communem divisorem, sequitur fieri non posse, ut sit

$$(4m-1)(4n-1)=1+aa.$$

Ergo non erit

$$16mn-4m-4n=aa;$$

unde ne eius quadrans quidem $4mn-m-n$ unquam quadratum esse potest.

1) Cf. § 20 Commentationis 134 huius voluminis. F. R.

2) Cf. § 68 huius Commentationis, imprimis notam adiectam. F. R.

THEOREMA 16

79. *Si in serie residuorum* 1, α, β, γ, δ *etc., quae ex divisione quadratorum per numerum quemcunque p resultant, cuiuspiam residui complementum in eadem serie residuorum occurrat, tum duo quadrata exhiberi poterunt, quorum summa sit per eundem numerum p divisibilis, etiamsi neutrum seorsim per p sit divisibile.*

DEMONSTRATIO

Praebeat quadratum aa residuum $= r$, quadratum autem bb residuum $= -r$ seu $p - r$, quod illius est complementum, ita ut r sit id residuum, cuius complementum simul in serie residuorum contineatur. Iam manifestum est summam horum quadratorum $aa + bb$ fore per numerum p divisibilem.

COROLLARIUM 1

80. Si p sit numerus primus, statim atque unius residui complementum in serie residuorum occurrit, etiam singulorum residuorum complementa ibidem inerunt. Sumto ergo quadrato quocunque aa, cuius residuum sit $= r$, dabitur aliud xx, cuius residuum erit $= -r$, ita ut x sit non maius quam $\frac{p}{2}$, atque summa $aa + xx$ erit per p divisibilis.

COROLLARIUM 2

81. Si igitur detur summa duorum quadratorum $aa + bb$ per numerum primum p divisibilis, quia residuorum ex aa et bb ortorum alterum alterius est complementum, residui ex quocunque alio quadrato cc orti complementum in serie residuorum quoque reperietur. Dabitur ergo summa duorum quadratorum $cc + xx$ per numerum p divisibilis.

COROLLARIUM 3

82. Ex praecedentibus autem patet hunc casum locum obtinere non posse, neque si p sit numerus [primus] formae $4n - 1$, neque si p saltem habeat factorem huius formae, quia neutro casu datur summa duorum quadratorum per p divisibilis, quae quidem quadrata sint inter se prima.

COROLLARIUM 4

83. Nulli ergo alii numeri primi relinquuntur, ad quos theorema hoc accommodari queat, nisi qui contineantur in hac forma $4n+1$.

SCHOLION

84. An autem omnes numeri primi formae $4n+1$ hanc habeant proprietatem, ut in seriebus residuorum inde ortis cuiusque termini complementum simul ibidem reperiatur, hic nondum est demonstratum neque desperandum videtur, quin ex his iisdem principiis demonstratio elici queat, etsi nondum mihi quidem eo pertingere licuit. Series autem residuorum ex simplicioribus numeris primis huius formae ortae sequenti modo se habent, ubi quidem residua semisse cuiusque numeri maiora per numeros negativos exhibere visum est, quo facilius, quaenam sint aliorum complementa, appareat:

$$5\,(1,\,-1),\quad 13\,(1,\,4,\,-4,\,3,\,-1,\,-3),\quad 17\,(1,\,4,\,-8,\,-1,\,8,\,2,\,-2,\,-4),$$
$$29\,(1,\,4,\,9,\,-13,\,-4,\,7,\,-9,\,6,\,-6,\,13,\,5,\,-1,\,-5,\,-7),$$
$$37\,(1,4,9,16,\,-12,\,-1,\,12,\,-10,\,7,\,-11,\,10,\,-4,\,-16,\,11,\,3,\,-3,\,-7,\,-9).$$

In his igitur seriebus perspicuum est cuiusque termini complementum simul in iis occurrere. Quod autem hoc necessario eveniat, si divisor sit numerus primus formae $4n+1$, demonstratio directa adhuc desideratur, quae hoc modo institui debere videtur. Prodeat ex numero primo $4n+1$ haec series residuorum $1, \alpha, \beta, \gamma, \delta$ etc., quorum terminorum numerus est $2n$; iam si quis neget horum terminorum complementa simul in eadem serie contineri, is dicere debet omnia complementa $-1, -\alpha, -\beta, -\gamma, -\delta$ etc. seriem non-residuorum constituere; quorum terminorum numerus cum sit $=2n$, sequeretur nulla alia praeterea dari non-residua; quare si assignari posset quispiam numerus in serie non-residuorum contentus, qui non esset complementum cuiuspiam termini in serie residuorum contenti, simul sequeretur nullum plane complementum seriei residuorum in serie non-residuorum occurrere. Hoc ergo si demonstrari posset, haberetur demonstratio desiderata et quidem directa. Nam demonstratio indirecta iam inde datur, quod demonstravi omnem numerum primum formae $4n+1$ esse summam duorum quadratorum; quare si sit $4n+1=aa+bb$, residuorum ex his quadratis aa et bb ortorum alterum alterius erit complementum hincque porro recte concluditur cuiusque residui complementum simul in serie residuorum contineri.

THEOREMA 17

85. *Si in serie residuorum* 1, α, β, γ, δ *etc., quae ex divisione quadratorum per numerum quemcunque* p *oriuntur, occurrat terminus, qui sit complementum summae duorum aliorum terminorum, tum summa trium quadratorum exhiberi potest per numerum* p *divisibilis, ita ut nullius quadrati radix maior sit quam* $\frac{p}{2}$.

DEMONSTRATIO

Sint r et s residua ex duobus quadratis aa et bb oriunda, quorum summa $= r + s$ eiusque ergo complementum $= p - r - s$ seu $-r - s$. Iam si hoc complementum in serie residuorum 1, α, β, γ, δ etc. reperiatur, dabitur quadratum $cc < \frac{1}{4}pp$, quod per p divisum relinquet $-r-s$; sicque manifestum erit summam horum trium quadratorum $aa + bb + cc$ fore per numerum p divisibilem neque horum quadratorum ullum maius esse quam $\frac{1}{4}pp$.

COROLLARIUM 1

86. Si igitur in serie residuorum 1, α, β, γ, δ etc. occurrat aliquis ex his numeris -2, $-1-\alpha$, -2α, $-1-\beta$, $-\alpha-\beta$, -2β, $-1-\gamma$, $-\alpha-\gamma$, $-\beta-\gamma$, -2γ, $-1-\delta$, $-\alpha-\delta$ etc., semper summa trium quadratorum exhiberi potest per numerum p divisibilis.

COROLLARIUM 2

87. Atque si p sit numerus primus, singulorum horum quadratorum radices a, b, c, cum sint minores quam $\frac{p}{2}$, erunt numeri ad p primi ideoque etiam ipsa quadrata; ac nisi ipsa haec tria quadrata fuerint prima inter se, sed communem habeant divisorem quadratum, quia hic necessario est ad p primus, per eum quadrata illa reducentur ad minora et prima inter se, quorum summa pariter per p erit divisibilis.

COROLLARIUM 3

88. Si in serie residuorum singulorum terminorum complementa simul insint, tum etiam summa duorum quadratorum assignari potest per numerum

p divisibilis. Quando autem duorum quadratorum summa datur, multo magis dabitur summa trium quadratorum, cum forma $aa + bb$ contineatur in forma $aa + bb + cc$.

SCHOLION

89. Simili modo demonstratur, si in serie residuorum occurrat numerus, qui sit complementum summae trium residuorum, tum summam quatuor quadratorum exhiberi posse, quae sit per numerum p divisibilis. Verum si summae binorum vel ternorum residuorum capiantur, tot prodeunt numeri diversi, ut satis manifestum videatur eorum omnium complementa in serie non-residuorum contineri non posse.

THEOREMA 18

90. *Proposito quocunque numero primo p si non duorum quadratorum inter se primorum summa per eum divisibilis exhiberi potest, certo semper summa trium quadratorum per eum divisibilis assignari potest, ita ut non singula seorsim per p sint divisibilia.*

DEMONSTRATIO

Sit $1, \alpha, \beta, \gamma, \delta, \varepsilon$ etc. series residuorum ex divisione quadratorum per numerum propositum primum p orta. Iam in hac serie vel occurrit -1 vel non occurrit. Si -1 ibi occurrit, singulorum residuorum complementa simul ibi occurrunt ideoque pluribus modis summa duorum quadratorum per p divisibilis datur. Sin autem -1 non in serie residuorum contineatur, in serie non-residuorum reperietur, ubi simul complementa omnium residuorum occurrent; hoc ergo casu nulla dabitur summa duorum quadratorum per numerum p divisibilis, nisi utrumque seorsim divisorem admittat. Dari autem his casibus summam trium quadratorum per numerum primum p divisibilem ita ostendo.

Primo notetur, si quis numerus r in serie residuorum occurrat, eius complementum $-r$ certo in serie non-residuorum esse, et vicissim si r sit non-residuum, certo fore $-r$ residuum. Ponamus iam negari ullam dari summam trium quadratorum per p divisibilem; et quia in serie residuorum primo adest numerus 1, numerus -2 ibidem non occurret (alias enim daretur summa trium quadratorum per p divisibilis contra hypothesin). Occurret igitur -2 in serie non-residuorum ac propterea numerus $+2$ in serie residuorum. Iam

cum in serie residuorum habeantur numeri 1 et 2, summae eorum complementum -3 erit non-residuum ideoque $+3$ residuum. Eodem modo ex residuis 1 et 3 concluditur fore -4 non-residuum ac proinde $+4$ residuum. Atque in genere si residuum quodcunque sit r, debebit $-r-1$ esse non-residuum hincque $1+r$ foret residuum. Ex hac ergo hypothesi sequitur omnes plane numeros 1, 2, 3, 4, 5, 6 etc. in serie residuorum contineri sicque nullos plane numeros pro serie non-residuorum relinqui; quod cum sit absurdum, concludere debemus dari utique trium quadratorum summam per numerum primum p divisibilem, quorum quidem nullum seorsim sit per p divisibile. Quae si forte non fuerint prima inter se, per eorum maximum communem divisorem ad prima deprimi poterunt, quia maximus communis divisor quadratorum certo est quadratus.

COROLLARIUM 1

91. Simili ratiocinio evincitur multo magis repugnare, si quis negaret dari quatuor quadratorum summam per numerum primum divisibilem. Ergo proposito numero quocunque primo p semper dabitur summa quatuor quadratorum per eum divisibilis.

COROLLARIUM 2

92. Si numerus primus p non sit divisor ullius summae duorum quadratorum, tria illa quadrata aa, bb, cc, quorum summa $aa+bb+cc$ est per p divisibilis, singula erunt minora quam $\frac{1}{4}pp$. Hinc ergo erit $aa+bb+cc<\frac{3}{4}pp$, unde quotus, qui ex divisione huius aggregati $aa+bb+cc$ per p oritur, erit $<\frac{3}{4}p$.

THEOREMA 19

93. *Si summa quatuor quadratorum per summam quatuor quadratorum dividatur, quotus erit quoque summa quatuor quadratorum saltem in fractis.*

DEMONSTRATIO

Sit $aa+bb+cc+dd$ summa quatuor quadratorum, quae dividenda sit per hanc summam quatuor quadratorum $pp+qq+rr+ss$; erit quotus

$$=\frac{aa+bb+cc+dd}{pp+qq+rr+ss},$$

qui, sive sit numerus integer sive fractus, semper in quatuor quadrata saltem in fractis resolvi potest. Multiplicemus enim numeratorem et denominatorem per $pp+qq+rr+ss$, ut denominator fiat quadratus; erit quotus iste

$$=\frac{(aa+bb+cc+dd)(pp+qq+rr+ss)}{(pp+qq+rr+ss)^2};$$

quodsi iam numerator in quatuor quadrata resolvi queat, ipsa fractio aequabitur aggregato quatuor quadratorum. At numerator pluribus modis in quatuor quadrata resolvi potest; si enim ponatur

$$(aa+bb+cc+dd)(pp+qq+rr+ss)=xx+yy+zz+vv,$$

erit

$$x=ap+bq+cr+ds,$$
$$y=aq-bp\pm cs\mp dr,$$
$$z=ar\mp bs-cp\pm dq,$$
$$v=as\pm br\mp cq-dp,\text{ [1]}$$

qui quatuor numeri, si singuli dividantur per communem denominatorem $pp+qq+rr+ss$, dabunt radices quatuor quadratorum, quorum summa aequatur quoto proposito. Nisi igitur hi numeri x, y, z et v sint divisibiles per $pp+qq+rr+ss$, saltem in fractis assignari possunt quatuor quadrata, quorum summa aequalis est quoto $\frac{aa+bb+cc+dd}{pp+qq+rr+ss}$.

COROLLARIUM 1

94. Quae hic de quatuor quadratorum summis sunt demonstrata, etiam ad summas trium vel etiam duorum patent, cum nihil impediat, quominus unus vel duo ex numeris a, b, c, d et p, q, r, s sint aequales nihilo.

COROLLARIUM 2

94[a].[2]) Si igitur summa trium quadratorum per summam quatuor vel etiam trium quadratorum dividatur, quotus certe erit summa quatuor quadratorum.

1) Hanc celebrem relationem EULERUS primum epistola d. 4. Maii 1748 scripta cum CHR. GOLDBACH communicavit. Vide *Correspondance math. et phys. publiée par P. H. Fuss*, St.-Pétersbourg 1843, t. I, p. 450; *LEONHARDI EULERI Opera omnia*, series III. F. R.

2) In editione principe falso numerus 94 iteratur. F. R.

COROLLARIUM 3

95. Quia productum ex duabus summis quatuor quadratorum est quoque summa quatuor quadratorum, patet, si omnes numeri primi sint summae quatuor quadratorum vel etiam pauciorum, tum etiam omnes omnino numeros esse summas quatuor quadratorum vel etiam pauciorum.

SCHOLION

96. Si summa quatuor quadratorum $aa+bb+cc+dd$ fuerit divisibilis per summam quatuor quadratorum $pp+qq+rr+ss$, tum quotum non solum in fractis, sed etiam in integris esse summam quatuor quadratorum est theorema elegantissimum FERMATII[1]), cuius demonstratio cum ipso nobis est erepta. Fateor me adhuc hanc demonstrationem invenire non potuisse, verumtamen hinc via aperitur ad theorema sequens demonstrandum, quo quilibet numerus summa quatuor quadratorum vel pauciorum asseritur, casu scilicet, quo quadrata fracta non excluduntur; etsi enim hoc theorema in integris quoque semper verum sit[2]), tamen non parum mihi praestitisse videor, quod id semota quadratorum integrorum ratione demonstraverim. Cum enim demonstratio adhuc post FERMATIUM sit frustra indagata, me proxime ad hunc scopum pertigisse arbitror.

THEOREMA 20

97. *Omnis numerus est summa quatuor quadratorum vel etiam pauciorum, siquidem quadrata fracta non excludantur.*

DEMONSTRATIO

Theorema hoc quidem verum est, etiamsi quadrata fracta excludantur; FERMATIUS enim affirmat omnem numerum integrum esse aggregatum ex

1) Sed vide notam 4 p. 358. F. R.

2) Hoc BACHETI theorema etiam in integris semper verum esse primum demonstravit I. L. LAGRANGE in Commentatione: *Démonstration d'un théorème d'arithmétique*, Nouv. mém. de l'acad. d. sc. de Berlin (1770), 1772, p. 123; *Oeuvres de Lagrange*, publiées par les soins de M. I.-A. SERRET, t. III, p. 189. Hac dissertatione provocatus EULERUS demonstrationem alteram dedit in Commentatione 445 (indicis ENESTROEMIANI): *Novae demonstrationes circa resolutionem numerorum in quadrata*, Nova acta erud. 1773, p. 193; *Leonhardi Euleri Opera omnia*, series I, vol. 3. F. R.

quatuor quadratis integris vel etiam paucioribus, ego autem fateor me hanc demonstrationem nondum invenire potuisse; dabo ergo demonstrationem pro casu, quo quadrata fracta non excluduntur. Iam notavi hanc demonstrationem tantum ad numeros primos reduci, de quibus ergo sufficit theorema demonstrasse. Quoniam igitur novimus numeros primos minores, ut 2, 3, 5, 7, 11, 13 etc., omnes in quatuor vel pauciora quadrata resolvi posse, si quis id de sequentibus neget, ei dicendum est dari aliquem numerum primum minimum, qui non sit summa quatuor pauciorumve quadratorum. Sit p iste numerus primus, ita ut omnes numeri primi ipso minores hincque etiam omnes compositi certo sint summae quatuor pauciorumve quadratorum. Iam per theorema praecedens datur summa trium quadratorum, quae sit $aa+bb+cc$, divisibilis per numerum istum p, ita ut singula haec quadrata sint minora quam $\frac{1}{4}pp$; unde erit

$$aa+bb+cc<\frac{3}{4}pp.$$

Quotus ergo

$$\frac{aa+bb+cc}{p}$$

erit minor quam $\frac{3}{4}p$; qui cum idcirco minor sit quam p, certe erit summa quatuor pauciorumve quadratorum; sit $xx+yy+zz+vv$ iste quotus; erit

$$p=\frac{aa+bb+cc}{xx+yy+zz+vv}$$

ideoque ipse numerus p erit summa quatuor pauciorumve quadratorum, quae in fractionibus etiam assignari possunt. Cum igitur inter numeros primos non detur minimus, qui in quatuor vel pauciora quadrata dispertiri nequeat, nullus prorsus datur numerus primus, qui non esset aggregatum quatuor pauciorumve quadratorum; quod cum certum sit de numeris primis, etiam valebit de omnibus numeris compositis ideoque de omnibus omnino numeris, ita ut nullus omnino detur numerus, qui non sit summa quatuor pauciorumve quadratorum.

COROLLARIUM 1

98. Cum omnis numerus integer sit summa quatuor pauciorumve quadratorum, eadem proprietas etiam ad omnes numeros fractos patet. Sit enim proposita fractio quaecunque $\frac{m}{n}$, quae transformetur in $\frac{mn}{nn}$. Iam sit $mn=\frac{aa}{pp}+\frac{bb}{qq}+\frac{cc}{rr}+\frac{dd}{ss}$ eritque

$$\frac{mn}{nn} = \frac{m}{n} = \frac{aa}{nnpp} + \frac{bb}{nnqq} + \frac{cc}{nnrr} + \frac{dd}{nnss};$$

ideoque omnis numerus fractus erit summa quatuor pauciorumve quadratorum.

COROLLARIUM 2

99. Quoniam, si de resolutione numerorum fractorum in quadrata sermo est, conditio illa quadratorum integrorum sponte evanescit, theorema in latiori sensu ita acceptum, ut omnes plane numeros, sive integros sive fractos, in quatuor vel pauciora quadrata resolubiles dicamus, sine ulla restrictione rigide demonstravi.

SCHOLION

100. Cum igitur FERMATIUS affirmasset omnem numerum integrum esse summam vel quatuor vel pauciorum quadratorum integrorum, nunc quidem hoc est demonstratum de quadratis in genere spectatis, fractis non exclusis. Quare ut FERMATIO satisfiat, superest, ut demonstremus, qui numerus integer in quatuor quadrata fracta resolvi queat, eundem quoque in quatuor vel pauciora quadrata integra resolvi posse. In Analysi quidem DIOPHANTEA pro certo assumi solet nullum numerum integrum in quatuor quadrata fracta dispertiri posse, nisi eius resolutio in quatuor quadrata integra vel pauciora constet; quod ergo si demonstratione esset confirmatum, nihil foret amplius desiderandum. Verum nusquam adhuc eiusmodi demonstrationem inveni. Quod autem ad theorema latissime patens attinet his verbis conceptum:

Omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum,

eius demonstrationem hic tradidi ita rigorosam, ut in ea nihil plane desiderari queat; hocque ipso non contemnendam partem demonstrationum FERMATIANARUM deperditarum mihi equidem videor restituisse.

OBSERVATIO DE SUMMIS DIVISORUM[1]

Commentatio 243 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 5 (1754/5), 1760, p. 59—74
Summarium ibidem p. 7—11

SUMMARIUM

Divisores cuiusque numeri ii vocantur numeri, per quos illum sine residuo dividere licet; unde inter divisores cuiusque numeri reperitur primo unitas, tum vero ille ipse numerus, quandoquidem omnis numerus tam per unitatem quam per se ipsum dividi potest. Iam constat eos numeros, qui praeter unitatem et se ipsos nullos alios divisores admittunt, vocari primos, reliquos vero, qui praeterea per alios numeros dividi se sine residuo patiuntur, compositos; atque in Arithmetica vulgari traditur methodus omnes cuiusque numeri divisores inveniendi. Auctor igitur in hac dissertatione summam omnium divisorum cuiusque numeri contemplatur, non eo consilio, uti alias in investigatione numerorum perfectorum vel amicabilium aliarumve huiusmodi quaestionum fieri solet, sed ut ordinem et quasi legem, qua istae summae divisorum singulis numeris convenientes procedant, exploret, qui certe maxime absconditus videri debet, cum pro numeris primis summa divisorum ipsos unitate superet, pro compositis autem eo magis, quo plures factores primos in se complectuntur. Quoniam igitur ratio progressionis numerorum primorum adhuc summum est mysterium, in quod ne FERMATIO quidem penetrare licuit, horum autem ratio manifesto in summas divisorum ingreditur, quis dubitaret has quoque nulli legi subiectas pronunciare? Eo maiorem igitur haec dissertatio attentionem meretur, quod ita lex ibi in lucem est protracta, etsi nondum summo rigore demonstrata. Auctori autem hic idem usu evenit, quod ante in theoremate FERMATIANO, ut mox deinceps defectum demonstrationis suppleverit. Quod enim in demonstratione hic tradita adhuc desideratur, statim in sequenti dissertatione supplebitur.

---

1) Vide Commentationes **152**, **175**, **244** huius voluminis. F. R.

Quo haec clarius exponi possint, utitur Auctor signo $\int$ ad summam divisorum cuiusque numeri, cui praefigitur, indicandam. Ita $\int n$ indicat summam omnium divisorum numeri n, unde intelligitur fore, ut sequitur:

$$\begin{array}{ll}
\int 1 = 1, & \int 11 = 1 + 11 = 12, \\
\int 2 = 1 + 2 = 3, & \int 12 = 1 + 2 + 3 + 4 + 6 + 12 = 28, \\
\int 3 = 1 + 3 = 4, & \int 13 = 1 + 13 = 14, \\
\int 4 = 1 + 2 + 4 = 7, & \int 14 = 1 + 2 + 7 + 14 = 24, \\
\int 5 = 1 + 5 = 6, & \int 15 = 1 + 3 + 5 + 15 = 24, \\
\int 6 = 1 + 2 + 3 + 6 = 12, & \int 16 = 1 + 2 + 4 + 8 + 16 = 31, \\
\int 7 = 1 + 7 = 8, & \int 17 = 1 + 17 = 18, \\
\int 8 = 1 + 2 + 4 + 8 = 15, & \int 18 = 1 + 2 + 3 + 6 + 9 + 18 = 39, \\
\int 9 = 1 + 3 + 9 = 13, & \int 19 = 1 + 19 = 20, \\
\int 10 = 1 + 2 + 5 + 10 = 18, & \int 20 = 1 + 2 + 4 + 5 + 10 + 20 = 42
\end{array}$$

etc.,

quae summae ex cognito principio, quod summa divisorum producti $mnpq$, cuius factores m, n, p, q fiant inter se numeri primi, aequalis sit producto ex summis divisorum singulorum seu

$$\int mnpq = \int m \cdot \int n \cdot \int p \cdot \int q,$$

pro maximis numeris facile definiri possunt. Ita est

$$\int 20 = \int 4 \cdot 5 = \int 4 \cdot \int 5 = 7 \cdot 6 = 42 \quad \text{et} \quad \int 360 = \int 8 \cdot 9 \cdot 5 = \int 8 \cdot \int 9 \cdot \int 5 = 15 \cdot 13 \cdot 6 = 1170.$$

Considerat autem Auctor has divisorum summas, prout secundum ordinem numerorum naturalem, quibus respondent, progrediuntur hoc modo:

numeri	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,	13,	14,	15,	16	etc.,
summae div.	1,	3,	4,	7,	6,	12,	8,	15,	13,	18,	12,	28,	14,	24,	24,	31	etc.,

in qua progressione certe nulla lex spectatur, cum modo sint maiores modo minores, modo pares modo impares, atque imprimis ordo numerorum primorum ei manifesto immiscetur; qui cum sit imperscrutabilis, quis in hac serie legem suspicaretur? Interim tamen Auctor docet hos numeros constituere seriem eius generis, quae recurrentes dici solent, ita ut quilibet eius terminus ex aliquot praecedentibus secundum certam quandam legem determinetur. Quemadmodum enim $\int n$ denotat summam divisorum numeri n, ita haec scriptura $\int (n - a)$ denotabit summam divisorum numeri $n - a$, quo observato lex illa ab Auctore inventa ita se habet, ut sit

$$\int n = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \int(n-15) \\ - \int(n-22) - \int(n-26) + \int(n-35) + \int(n-40) - \text{etc.},$$

ubi ratione signorum tenendum est semper bina + excipi a binis —; numeri autem 1, 2, 5, 7, 12, 15 etc. continuo ab n subtrahendi ex differentiis facile cognoscuntur:

numeri	1,	2,	5,	7,	12,	15,	22,	26,	35,	40,	51,	57 etc.,
differ.	1,	3,	2,	5,	3,	7,	4,	9,	5,	11,	6 etc.,	

dummodo alternatim summantur. Commodius igitur illa relatio ita repraesentabitur:

$$\int n = \begin{cases} +\int(n-1) - \int(n-5) + \int(n-12) - \int(n-22) + \int(n-35) - \text{etc.} \\ +\int(n-2) - \int(n-7) + \int(n-15) - \int(n-26) + \int(n-40) - \text{etc.} \end{cases}$$

Pro applicatione autem huius formulae ad quosvis numeros sciendum est hos terminos eousque tantum sumi debere, quoad numeri post signum $\int$ scripti fiant negativi, qui omnes sunt omittendi; tum vero, si occurrat terminus $\int(n-n)$ seu $\int 0$, quia hic per se non determinatur, quovis casu eius loco ipsum numerum n scribi oportere. Per hanc ergo legem erit

$$\int 21 = \int 20 + \int 19 - \int 16 - \int 14 + \int 9 + \int 6$$

seu

$$\int 21 = 42 + 20 - 31 - 24 + 13 + 12 = 87 - 55 = 32;$$

tum

$$\int 22 = \int 21 + \int 20 - \int 17 - \int 15 + \int 10 + \int 7 - \int 0$$

seu

$$\int 22 = 32 + 42 - 18 - 24 + 18 + 8 - 22 = 100 - 64 = 36.$$

Ad hanc mirabilem progressionis legem deductus est Auctor consideratione huius producti

$$(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7) \text{ etc.},$$

cuius factores in infinitum progredi concipiuntur; quod si per actualem multiplicationem evolvatur, observavit prodire hanc seriem

$$1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + \text{etc.},$$

quousque scilicet operationem actu continuare licuit, unde legem huius seriei et exponentium progressionem tantum per inductionem conclusit, quod forte pluribus sufficere videatur. Verum Auctor ingenue fatetur hanc observatam convenientiam minime adhuc esse demonstratam, sed eius demonstrationem etiamnum desiderari, quam autem haud multo post cum Academia communicavit. Concessa autem aequalitate illius producti et seriei evolutae theorema memoratum circa ordinem in summis divisorum perspicue inde demonstratur, ut

nullum amplius dubium superesse possit, etiamsi logarithmis et differentiatione sit opus, quae res parum ad naturam divisorum pertinere videantur. Ex hoc ergo casu intelligere licet, quam arcto et mirifico nexu Analysis infinitorum non solum cum Analysi vulgari, sed etiam cum doctrina numerorum, quae ab hoc sublimi calculi genere abhorrere videtur, sit coniuncta.

1. Proposito quocunque numero n denotet haec formula $\int n$ summam omnium divisorum numeri n. Ita cum unitas praeter se ipsam alium non habeat divisorem, erit $\int 1 = 1$; atque cum numerus primus duos tantum habeat divisores, unitatem et se ipsum, si n fuerit numerus primus, erit $\int n = 1 + n$. Deinde cum numerus perfectus aequalis sit summae suarum partium aliquotarum, partes aliquotae autem sint divisores eius praeter ipsum numerum, manifestum est numeri perfecti summam divisorum se ipso esse duplo maiorem; hinc si n sit numerus perfectus, erit $\int n = 2n$. Porro quoniam numerus redundans appellari solet is, cuius summa partium aliquotarum ipso est maior, si n sit numerus redundans, erit $\int n > 2n$; ac si n sit numerus deficiens seu talis, cuius summa partium aliquotarum ipso est minor, erit $\int n < 2n$.

2. Hoc igitur modo indoles numerorum, quatenus summa partium aliquotarum vel divisorum continetur, facile signis exprimitur. Si enim fuerit $\int n = 1 + n$, erit n numerus primus, si sit $\int n = 2n$, erit n numerus perfectus, ac si sit vel $\int n > 2n$ vel $\int n < 2n$, numerus n erit vel redundans vel deficiens. Huc etiam referri potest quaestio de numeris, qui amicabiles vocari solent, quorum alter summae partium aliquotarum alterius aequatur. Si enim sint m et n numeri amicabiles, cum numeri m sit summa partium aliquotarum $= \int m - m$ et numeri $n = \int n - n$, erit ex natura horum numerorum $n = \int m - m$ et $m = \int n - n$ sicque habebitur $\int m = \int n = m + n$. Duo ergo numeri amicabiles eandem divisorum summam habent, quae simul summae amborum numerorum est aequalis.

3. Quo summa divisorum cuiusque numeri propositi facilius inveniri possit, id commodissime fiet hunc numerum in duos factores, qui inter se sint primi, resolvendo. Si enim sint p et q numeri inter se primi seu qui praeter unitatem nullum habeant divisorem communem, tum summa divi-

sorum producti pq aequale erit producto ex summis divisorum utriusque seu erit

$$\int pq = \int p \cdot \int q.$$

Hinc inventis summis divisorum numerorum minorum inventio summae divisorum non difficulter ad numeros maiores extenditur.

4. Si sint a, b, c, d etc. numeri primi, omnis numerus, quantuscunque fuerit, semper ad huiusmodi formam $a^\alpha b^\beta c^\gamma d^\delta$ etc. reducitur; qua forma inventa erit huius numeri summa divisorum seu $\int a^\alpha b^\beta c^\gamma d^\delta$ etc.

$$= \int a^\alpha \cdot \int b^\beta \cdot \int c^\gamma \cdot \int d^\delta \cdot \text{etc.}$$

At ob a, b, c, d etc. numeros primos erit

$$\int a^\alpha = 1 + a + a^2 + \cdots + a^\alpha = \frac{a^{\alpha+1}-1}{a-1}$$

ideoque

$$\int a^\alpha b^\beta c^\gamma d^\delta \text{ etc.} = \frac{a^{\alpha+1}-1}{a-1} \cdot \frac{b^{\beta+1}-1}{b-1} \cdot \frac{c^{\gamma+1}-1}{c-1} \cdot \frac{d^{\delta+1}-1}{d-1} \cdot \text{etc.}^{1)}$$

Sufficiet ergo singularum potestatum numerorum primorum tantum summas divisorum invenisse.

5. Hanc autem indagationem ulterius non persequor, sed ut ad id, quod hic tractare institui, propius accedam, numerorum secundum ordinem naturalem progredientium summas divisorum hic conspectui exponam.

$\int 1 = 1$	$\int 5 = 6$	$\int 9 = 13$	$\int 13 = 14$	$\int 17 = 18$
$\int 2 = 3$	$\int 6 = 12$	$\int 10 = 18$	$\int 14 = 24$	$\int 18 = 39$
$\int 3 = 4$	$\int 7 = 8$	$\int 11 = 12$	$\int 15 = 24$	$\int 19 = 20$
$\int 4 = 7$	$\int 8 = 15$	$\int 12 = 28$	$\int 16 = 31$	$\int 20 = 42$

1) Has relationes, quae etiam inveniuntur in Commentationibus 152 et 175 huius voluminis, iam a Fr. v. Schooten et I. Wallis (in alia quidem forma) traditas esse annotavit G. Eneström, Biblioth. Mathem. 6_3, 1905, p. 408. Vide Fr. v. Schooten, *Exercitationum mathematicarum libri quinque,* Lugd. Batav. 1657, libri V sectio I, p. 378—380, et I. Wallis, *A treatise of Algebra,* London 1685 (Additional Treatise of Combinations etc., p. 122). F. R.

$\int 21 = 32$	$\int 37 = 38$	$\int 53 = 54$	$\int 69 = 96$	$\int 85 = 108$
$\int 22 = 36$	$\int 38 = 60$	$\int 54 = 120$	$\int 70 = 144$	$\int 86 = 132$
$\int 23 = 24$	$\int 39 = 56$	$\int 55 = 72$	$\int 71 = 72$	$\int 87 = 120$
$\int 24 = 60$	$\int 40 = 90$	$\int 56 = 120$	$\int 72 = 195$	$\int 88 = 180$
$\int 25 = 31$	$\int 41 = 42$	$\int 57 = 80$	$\int 73 = 74$	$\int 89 = 90$
$\int 26 = 42$	$\int 42 = 96$	$\int 58 = 90$	$\int 74 = 114$	$\int 90 = 234$
$\int 27 = 40$	$\int 43 = 44$	$\int 59 = 60$	$\int 75 = 124$	$\int 91 = 112$
$\int 28 = 56$	$\int 44 = 84$	$\int 60 = 168$	$\int 76 = 140$	$\int 92 = 168$
$\int 29 = 30$	$\int 45 = 78$	$\int 61 = 62$	$\int 77 = 96$	$\int 93 = 128$
$\int 30 = 72$	$\int 46 = 72$	$\int 62 = 96$	$\int 78 = 168$	$\int 94 = 144$
$\int 31 = 32$	$\int 47 = 48$	$\int 63 = 104$	$\int 79 = 80$	$\int 95 = 120$
$\int 32 = 63$	$\int 48 = 124$	$\int 64 = 127$	$\int 80 = 186$	$\int 96 = 252$
$\int 33 = 48$	$\int 49 = 57$	$\int 65 = 84$	$\int 81 = 121$	$\int 97 = 98$
$\int 34 = 54$	$\int 50 = 93$	$\int 66 = 144$	$\int 82 = 126$	$\int 98 = 171$
$\int 35 = 48$	$\int 51 = 72$	$\int 67 = 68$	$\int 83 = 84$	$\int 99 = 156$
$\int 36 = 91$	$\int 52 = 98$	$\int 68 = 126$	$\int 84 = 224$	$\int 100 = 217.$

6. Si iam contemplemur seriem horum numerorum 1, 3, 4, 7, 6, 12, 8, 15, 13, 18, 12, 28 etc., quam summae divisorum numeris naturali ordine procedentibus respondentes constituunt, non solum nulla lex progressionis patet, sed ordo horum numerorum tantopere est perturbatus, ut nulli prorsus legi adstrictus videatur. Quin etiam haec series ordinem numerorum primorum manifesto implicat, cum terminus indicis n seu $\int n$ toties sit $= n + 1$, quoties n est numerus primus; constat autem numeros primos nullo adhuc modo ad certam quandam progressionis legem revocari potuisse. Cum autem nostra series non solum numerorum primorum, sed etiam omnium reliquorum numerorum, quatenus ex primis sunt compositi, rationem complectatur, eius lex multo etiam difficilior inventu videtur quam ipsius seriei numerorum primorum.

7. Quae cum ita sint, non parum equidem mihi scientiam numerorum promovisse videor, dum certam atque constantem legem detexi, secundum quam termini seriei propositae 1, 3, 4, 7, 6 etc. progrediantur, ita ut per hanc legem quilibet istius seriei terminus ex praecedentibus definiri possit; inveni enim, quod magis mirum videatur, hanc seriem ad id genus progressionum pertinere, quae recurrentes vocari solent et quarum natura ita est comparata, ut quilibet terminus ex praecedentibus secundum certam quandam relationis rationem determinetur. Quis autem unquam crediderit hanc seriem tantopere perturbatam et quae cum seriebus recurrentibus nihil plane commune habere videtur, nihilominus in hoc serierum genere contineri eiusque scalam relationis assignari posse?

8. Cum huius seriei terminus indici n respondens, qui indicat summam divisorum numeri n, sit $=\int n$, eius termini antecedentes ordine retrogrado erunt $\int(n-1)$, $\int(n-2)$, $\int(n-3)$, $\int(n-4)$, $\int(n-5)$ etc. Quilibet autem terminus istius seriei, scilicet $\int n$, ita ex aliquot antecedentium conflatur, ut sit[1])

$$\begin{aligned}\int n = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \int(n-15)\\ - \int(n-22) - \int(n-26) + \int(n-35) + \int(n-40) - \int(n-51) - \int(n-57)\\ + \int(n-70) + \int(n-77) - \int(n-92) - \int(n-100) + \int(n-117) + \int(n-126) - \text{etc.}\end{aligned}$$

Vel cum signa $+$ et $-$ alternatim binos terminos afficiant, haec series commode in duas divellitur hoc modo:

$$\int n = \begin{cases} \int(n-1) - \int(n-5) + \int(n-12) - \int(n-22) + \int(n-35) - \int(n-51) + \text{etc.}\\ \int(n-2) - \int(n-7) + \int(n-15) - \int(n-26) + \int(n-40) - \int(n-57) + \text{etc.}\end{cases}$$

9. Ex hac posteriori forma ordo numerorum, qui in utraque serie successive a numero n subtrahuntur, facile perspicitur; utraque enim series est secundi ordinis differentias secundas habens constantes. Namque prioris seriei numeri cum suis differentiis tam primis quam secundis sunt

1) Vide p. 245. F. R.

	1,	5,	12,	22,	35,	51,	70,	92,	117	etc.,
diff. 1.	4,	7,	10,	13,	16,	19,	22,	25	etc.,	
diff. 2.	3,	3,	3,	3,	3,	3,	3	etc.		

Unde illius seriei terminus generalis est $= \frac{3xx-x}{2}$ continetque adeo omnes numeros pentagonales. Altera series est

	2,	7,	15,	26,	40,	57,	77,	100,	126	etc.,
diff. 1.	5,	8,	11,	14,	17,	20,	23,	26	etc.,	
diff. 2.	3,	3,	3,	3,	3,	3,	3	etc.		

ideoque terminum generalem habet $\frac{3xx+x}{2}$ ac seriem numerorum pentagonalium retro continuatam continet.

10. Omnino hic notatu est dignum seriem numerorum pentagonalium tam ipsam quam retro continuatam ad ordinem seriei summarum divisorum potissimum adhiberi, cum sane nullum nexum inter numeros pentagonales et summas divisorum ne suspicari quidem liceat. Si enim series numerorum pentagonalium tam antrorsum quam retrorsum continuata exponatur hoc modo

etc. 77, 57, 40, 26, 15, 7, 2, 0, 1, 5, 12, 22, 35, 51, 70, 92 etc.,

formula nostra ordinem summarum divisorum complectens signis alternantibus hoc modo ordinata exhiberi poterit

$$\text{etc.} - \int(n-15) + \int(n-7) - \int(n-2) + \int(n-0) - \int(n-1)$$
$$+ \int(n-5) - \int(n-12) + \int(n-22) - \text{etc.} = 0,$$

quae series utrinque quidem in infinitum excurrit, sed quovis casu, siquidem ad usum nostrum rite adhibeatur, determinato terminorum numero constat.

11. Si enim ope formulae nostrae primum exhibitae

$$\int n = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \int(n-15)$$
$$- \int(n-22) - \int(n-26) + \int(n-35) + \int(n-40) - \int(n-51) - \int(n-57)$$
$$+ \int(n-70) + \int(n-77) - \int(n-92) - \int(n-100) + \text{etc.}$$

summam divisorum numeri n invenire velimus ex cognitis divisorum summis numerorum minorum, plures terminos huius formulae accipere non oportet, quam quoad ad summas divisorum numerorum negativorum perveniatur. Omnes scilicet termini, qui post signum $\int$ numeros negativos continent, sunt reiiciendi; unde patet, si n sit numerus exiguus, paucissimos terminos sufficere, quo maior autem fuerit numerus n, eo plures terminos ex formula nostra generali ad usum adhiberi debere.

12. Summa igitur divisorum numeri propositi n ex summis divisorum aliquot numerorum minorum, quas cognitas esse assumo, conflatur, quoniam quovis casu summae numerorum negativorum reiiciuntur. Quae cautio cum eo sit facilior, quod numerorum negativorum summa divisorum ne concipi quidem possit, insuper moneri oportet, quomodo operatio sit dirigenda iis casibus, quibus formula nostra praebet terminum $\int(n-n)$ seu $\int 0$, qui, cum cyphra per omnes numeros sit divisibilis, vel infinitus vel indeterminatus videtur. Casus hic autem toties occurrit, quoties n est numerus ex serie numerorum pentagonalium vel ipsa vel retro continuata; his igitur casibus tenendum est semper pro termino $\int(n-n)$ seu $\int 0$ ipsum illum numerum n, qui proponitur, esse scribendum et quidem cum eo signo, quo terminus $\int(n-n)$ in formula nostra afficitur.

13. His expositis praeceptis, quae ad usum formulae nostrae observari debent, exempla a numeris minimis inchoando apponam, quo facilius vis formulae nostrae perspiciatur simulque eius veritas agnoscatur.

$$\int 1 = \int 0$$

seu

$$\int 1 = \quad 1 \quad = 1$$

$$\int 2 = \int 1 + \int 0$$

seu

$$\int 2 = \quad 1 + \quad 2 = 3$$

$$\int 3 = \int 2 + \int 1$$

seu

$$\int 3 = \quad 3 + \quad 1 = 4$$

$$\int 4 = \int 3 + \int 2$$

seu

$$\int 4 = 4 + 3 = 7$$

$$\int 5 = \int 4 + \int 3 - \int 0$$

seu

$$\int 5 = 7 + 4 - 5 = 6$$

$$\int 6 = \int 5 + \int 4 - \int 1$$

seu

$$\int 6 = 6 + 7 - 1 = 12$$

$$\int 7 = \int 6 + \int 5 - \int 2 - \int 0$$

seu

$$\int 7 = 12 + 6 - 3 - 7 = 8$$

$$\int 8 = \int 7 + \int 6 - \int 3 - \int 1$$

seu

$$\int 8 = 8 + 12 - 4 - 1 = 15$$

$$\int 9 = \int 8 + \int 7 - \int 4 - \int 2$$

seu

$$\int 9 = 15 + 8 - 7 - 3 = 13$$

$$\int 10 = \int 9 + \int 8 - \int 5 - \int 3$$

seu

$$\int 10 = 13 + 15 - 6 - 4 = 18$$

$$\int 11 = \int 10 + \int 9 - \int 6 - \int 4$$

seu

$$\int 11 = 18 + 13 - 12 - 7 = 12$$

$$\int 12 = \int 11 + \int 10 - \int 7 - \int 5 + \int 0$$

seu

$$\int 12 = 12 + 18 - 8 - 6 + 12 = 28.$$

14. Exempla haec attentius inspicienti atque etiam ad numeros maiores progredienti non sine admiratione patebit, quemadmodum semper quasi praeter expectationem ad veram divisorum summam numeri propositi perveniatur; et quo hic consensus facilius deprehendatur, supra iam omnium numerorum centenario non maiorum summas divisorum exhibui, unde veritas

nostrae formulae in numeris maioribus explorari poterit. Imprimis autem non sine delectatione reperiemus, quoties numerus propositus fuerit primus, ex formula nostra pro eius divisorum summa inveniri numerum unitate maiorem. Evolvamus in hunc finem exemplum, quo numerus propositus $n = 101$, quasi ignorantes exploraturi, utrum hic numerus sit primus necne, atque operatio ita constabit:

$$\begin{array}{l} \int 101 = \int 100 + \int 99 - \int 96 - \int 94 + \int 89 + \int 86 - \int 79 - \int 75 \\ \qquad\quad 217 + 156 - 252 - 144 + 90 + 132 - 80 - 124 \\ + \int 66 + \int 61 - \int 50 - \int 44 + \int 31 + \int 24 - \int 9 - \int 1 \\ + 144 + 62 - 93 - 84 + 32 + 60 - 13 - 1. \end{array}$$

Colligendis ergo binis terminis erit

$$\begin{array}{rl} \int 101 = & + 373 - 396 \\ & + 222 - 204 \\ & + 206 - 177 \\ & + \ 92 - \ 14 \\ \hline \end{array}$$

seu

$$\int 101 = + 893 - 791 = 102.$$

Reperitur ergo summa divisorum numeri 101 unitate maior, scilicet 102, unde, etiamsi id aliunde non constaret, sequitur manifesto numerum 101 esse primum. Hoc autem merito eo mirabilius videtur, cum nulla operatio sit instituta, quae ad rationem divisorum ullo modo referri queat; quin etiam divisores, quorum summa per hanc regulam reperitur, ipsi manent incogniti, etiamsi saepe ex consideratione ipsius summae concludi possint.

15. Insignis haec proprietas, qua summae divisorum sunt praeditae, non minus foret memorabilis, etiamsi eius demonstratio esset obvia et quasi in aprico posita. Sin autem demonstratio admodum esset abstrusa atque numerorum proprietatibus maxime reconditis inniteretur, inde non mediocriter certe pretium huius legis progressionis repertae augeretur, siquidem earum veritatum investigatio eo magis est laudanda, quo magis eae fuerint absconditae. Verum dum fateri cogor me non solum nullam huius veritatis demonstrationem proferre posse, sed etiam propemodum pro desperato

habere, nescio, annon ob hanc ipsam causam cognitio talis veritatis multo magis sit aestimanda, cuius demonstratio nobis est imperscrutabilis. Atque hanc ob rem istam veritatem pluribus exemplis confirmare visum est, quod mihi quidem eius demonstrationem exhibere non liceat.

16. Eximium igitur hic eiusmodi propositionum habemus exemplum, de quarum veritate nullo modo dubitare possumus, etiamsi eas demonstrare non valeamus, quod plerisque eo magis mirum videbitur, quod in mathesi vulgo nullae aliae propositiones admitti putantur, nisi quarum veritas ex indubitatis principiis evinci queat. Interim tamen non fortuito et quasi divinando ad cognitionem huius veritatis perveni; cui enim in mentem venire potuisset ordinem, qui forte in summis divisorum locum habuerit, ex natura serierum recurrentium ac numerorum pentagonalium per solam coniecturam elicere velle? Hanc ob rem non abs re fore arbitror, si modum, quo ad cognitionem huius ordinis pertigerim, dilucide exposuero, praesertim cum is admodum sit reconditus ac longe multasque per ambages conquisitus.

17. Deductus autem sum ad hanc observationem per considerationem istius formulae infinitae

$$s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7)(1-x^8) \text{ etc.},$$

cuius valorem, si multiplicatione singulorum factorum actu instituta evolvatur ac secundum potestates ipsius x disponatur, deprehendi in sequentem seriem converti[1])

$$s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + x^{51} + x^{57} - \text{etc.},$$

ubi in exponentibus ipsius x iidem numeri occurrunt, quos supra descripsi, numeri scilicet pentagonales cum ipsi tum retro continuati. Unde, quo ordo facilius perspiciatur, haec series ita exhiberi poterit, ut utrinque in infinitum excurrat

$$s = \text{etc.} + x^{26} - x^{15} + x^7 - x^2 + x^0 - x^1 + x^5 - x^{12} + x^{22} - x^{35} + x^{51} - \text{etc.}$$

1) Vide notam p. 191. F. R.

18. Aequalitas harum duarum formularum pro s exhibitarum iam est id ipsum, quod solida demonstratione confirmare non possum; verumtamen qui opus evolutionis formulae prioris

$$s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5) \text{ etc.}$$

in se suscipere hosque factores successive in se multiplicare voluerit, statim ad terminos primores alterius seriei

$$s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \text{etc.}$$

perveniet neque difficulter perspiciet bina signa + et — geminata se invicem excipere et exponentes potestatum ipsius x eam legem sequi, quam iam satis exposui. Concessa autem hac aequalitate inter binas istas formulas infinitas proprietas summarum divisorum, quam ante indicavi, rigide inde demonstrari potest; atque vicissim si haec proprietas pro vera agnoscatur, ex ea veritas consensus duarum harum formularum evincetur.

19. Quodsi enim pro demonstrato assumamus posito

$$s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5) \text{ etc.}$$

fore

$$s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.},$$

erit logarithmis sumendis

$$ls = l(1-x) + l(1-x^2) + l(1-x^3) + l(1-x^4) + l(1-x^5) + \text{etc.}$$

et

$$ls = l(1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.}).$$

Sumantur utriusque formae differentialia eritque

$$\frac{ds}{s} = -\frac{dx}{1-x} - \frac{2x\,dx}{1-x^2} - \frac{3xx\,dx}{1-x^3} - \frac{4x^3dx}{1-x^4} - \frac{5x^4dx}{1-x^5} - \text{etc.}$$

et

$$\frac{ds}{s} = \frac{-dx - 2x\,dx + 5x^4dx + 7x^6dx - 12x^{11}dx - 15x^{14}dx + \text{etc.}}{1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.}}.$$

Multiplicetur utraque per $\frac{-x}{dx}$, ut habeatur

$$\text{I.}\quad -\frac{xds}{sdx}=\frac{x}{1-x}+\frac{2x^2}{1-x^2}+\frac{3x^3}{1-x^3}+\frac{4x^4}{1-x^4}+\frac{5x^5}{1-x^5}+\text{etc.},$$

$$\text{II.}\quad -\frac{xds}{sdx}=\frac{x+2x^2-5x^5-7x^7+12x^{12}+15x^{15}-22x^{22}-26x^{26}+\text{etc.}}{1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-\text{etc.}}.$$

20. Harum expressionum inter se aequalium contemplemur primo priorem ac singulos terminos more consueto in progressiones geometricas convertamus; quo facto prodibit infinitas has progressiones geometricas secundum potestates ipsius x disponendo:

$$
\begin{array}{rcccccccccccc}
-\frac{xds}{sdx}= & x^1+ & x^2+ & x^3+ & x^4+ & x^5+ & x^6+ & x^7+ & x^8+ & x^9+ & x^{10}+ & x^{11}+ & x^{12}+\text{etc.}\\
 & & +2 & & +2 & & +2 & & +2 & & +2 & & +2\\
 & & & +3 & & & +3 & & & +3 & & & +3\\
 & & & & +4 & & & & +4 & & & & +4\\
 & & & & & +5 & & & & & +5 & & \\
 & & & & & & +6 & & & & & & +6\\
 & & & & & & & +7 & & & & & \\
 & & & & & & & & +8 & & & & \\
 & & & & & & & & & +9 & & & \\
 & & & & & & & & & & +10 & & \\
 & & & & & & & & & & & +11 & \\
 & & & & & & & & & & & & +12
\end{array}
$$

21. Si iam singularum potestatum ipsius x coefficientes colligantur, habebitur

$$-\frac{xds}{sdx}=x^1+x^2(1+2)+x^3(1+3)+x^4(1+2+4)+x^5(1+5)+x^6(1+2+3+6)+\text{etc.},$$

ubi manifestum est cuiusque potestatis ipsius x coefficientem esse aggregatum omnium numerorum, per quos exponens illius potestatis est divisibilis. Scilicet potestatis x^n coefficiens erit summa omnium divisorum numeri n; erit ergo

is secundum modum signandi supra receptum $=\int n$. Hinc itaque series ipsi $-\frac{x\,ds}{s\,dx}$ aequalis inventa ita exhibebitur, ut sit

$$-\frac{x\,ds}{s\,dx}=x\int 1+x^2\int 2+x^3\int 3+x^4\int 4+x^5\int 5+x^6\int 6+x^7\int 7+\text{etc.},$$

sicque posito $x=1$ prodit progressio summarum divisorum, qui singulis numeris ordine naturali progredientibus conveniunt.

22. Designemus iam hanc seriem per t, ut sit

$$t=x^1\int 1+x^2\int 2+x^3\int 3+x^4\int 4+x^5\int 5+x^6\int 6+x^7\int 7+\text{etc.},$$

et ob $t=-\frac{x\,ds}{s\,dx}$ erit quoque

$$t=\frac{x^1+2x^2-5x^5-7x^7+12x^{12}+15x^{15}-22x^{22}-26x^{26}+\text{etc.}}{1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-\text{etc.}}.$$

Necesse igitur est, ut ex evolutione huius fractionis pro t series obtineatur aequalis illi, quam prior forma suppeditavit; unde manifestum est seriem illam pro t inventam esse recurrentem, cuius singuli termini per praecedentes determinentur secundum scalam relationis, quam denominator $1-x-x^2+x^5+x^7-\text{etc.}$ indicat.

23. Quo nunc facilius indoles huius seriei recurrentis cognoscatur, binos istos valores pro t inventos inter se coaequemus atque ad fractionem tollendam uterque per denominatorem $1-x-x^2+x^5+x^7-x^{12}-x^{15}+\text{etc.}$ multiplicetur, quo facto orietur terminis secundum potestates ipsius x disponendis

$$\begin{array}{llllllllllll}
x^1\int 1 & +x^2\int 2 & +x^3\int 3 & +x^4\int 4 & +x^5\int 5 & +x^6\int 6 & +x^7\int 7 & +x^8\int 8 & +x^9\int 9 & +x^{10}\int 10 & +x^{11}\int 11 & +x^{12}\int 12+\text{etc.}\\
 & -\int 1 & -\int 2 & -\int 3 & -\int 4 & -\int 5 & -\int 6 & -\int 7 & -\int 8 & -\int 9 & -\int 10 & -\int 11\\
 & & -\int 1 & -\int 2 & -\int 3 & -\int 4 & -\int 5 & -\int 6 & -\int 7 & -\int 8 & -\int 9 & -\int 10\\
 & & & & & +\int 1 & +\int 2 & +\int 3 & +\int 4 & +\int 5 & +\int 6 & +\int 7\\
 & & & & & & & +\int 1 & +\int 2 & +\int 3 & +\int 4 & +\int 5\\
 & & & & & & & & & & & \vdots
\end{array}$$

aequale

$$\begin{array}{llllllllllll}
x^1 & +2x^2 & * & * & -5x^5 & * & -7x^7 & * & * & * & * & +12x^{12}+\text{etc.}
\end{array}$$

24. Cum iam singularum postestatum ipsius x coefficientes se mutuo destruere debeant, hinc sequentes eliciemus aequalitates

$$\int 1 = 1, \qquad \int 7 = \int 6 + \int 5 - \int 2 - 7,$$
$$\int 2 = \int 1 + 2, \qquad \int 8 = \int 7 + \int 6 - \int 3 - \int 1,$$
$$\int 3 = \int 2 + \int 1, \qquad \int 9 = \int 8 + \int 7 - \int 4 - \int 2,$$
$$\int 4 = \int 3 + \int 2, \qquad \int 10 = \int 9 + \int 8 - \int 5 - \int 3,$$
$$\int 5 = \int 4 + \int 3 - 5, \qquad \int 11 = \int 10 + \int 9 - \int 6 - \int 4,$$
$$\int 6 = \int 5 + \int 4 - \int 1, \qquad \int 12 = \int 11 + \int 10 - \int 7 - \int 5 + 12$$

etc.,

quae manifesto redeunt ad istas

$$\int 1 = 1, \qquad \int 7 = \int(7-1) + \int(7-2) - \int(7-5) - 7,$$
$$\int 2 = \int(2-1) + 2, \qquad \int 8 = \int(8-1) + \int(8-2) - \int(8-5) - \int(8-7),$$
$$\int 3 = \int(3-1) + \int(3-2), \qquad \int 9 = \int(9-1) + \int(9-2) - \int(9-5) - \int(9-7),$$
$$\int 4 = \int(4-1) + \int(4-2), \qquad \int 10 = \int(10-1) + \int(10-2) - \int(10-5) - \int(10-7),$$
$$\int 5 = \int(5-1) + \int(5-2) - 5, \qquad \int 11 = \int(11-1) + \int(11-2) - \int(11-5) - \int(11-7),$$
$$\int 6 = \int(6-1) + \int(6-2) - \int(6-5), \qquad \int 12 = \int(12-1) + \int(12-2) - \int(12-5) - \int(12-7) + 12.$$

25. Hic perspicuum est numeros, qui continuo a numero proposito, cuius divisorum summa quaeritur, subtrahi debent, esse ipsos numeros seriei 1, 2, 5, 7, 12, 15, 22, 26 etc., ex quibus tot quovis casu sunt sumendi, quoad numerum propositum non excedant; atque etiam signa eam tenere rationem, quae supra est descripta. Hinc ergo proposito numero quocunque n manifestum est fore

$$\int n = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \int(n-15) - \text{etc.}$$

hos terminos eousque continuando, donec numeri signum $\int$ praefixum habentes fiant negativi. Simul ergo ex origine seriei huius recurrentis ratio patet, cur ista progressio quovis casu ulterius continuari non debeat.

26. Quod porro ad numeros absolutos attinet, qui in formularum inventarum aliquibus sub finem annectuntur, manifestum est eos ex numeratore fractionis, qua valor ipsius t expressus est inventus (§ 22), oriri atque iis tantum casibus legem continuitatis interrumpere, quibus numerus n est terminus huius seriei 1, 2, 5, 7, 12, 15, 22, 26 etc., quanquam ne hoc quidem casu lex signorum perturbatur. His autem casibus numerus absolutus insuper cum signo suo adiiciendus ipsi numero proposito est aequalis; atque si legem ante descriptam consideremus, hunc numerum utique deprehendemus respondere termino $\int(n-n)$, unde ratio patet, cur, quoties in applicatione formae

$$\int n = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \text{etc.}$$

pervenitur ad terminum $\int(n-n)$, is non omitti, sed pro eius valore ipse numerus n scribi debeat. Hinc igitur regula supra exposita in omnibus partibus confirmatur.

DEMONSTRATIO THEOREMATIS CIRCA ORDINEM IN SUMMIS DIVISORUM OBSERVATUM[1]

Commentatio 244 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 5 (1754/5), 1760, p. 75—83
Summarium ibidem p. 11

SUMMARIUM

Hic Cel. Auctor id, quod in praecedente dissertatione adhuc desiderabatur, cumulate praestat et demonstrationem convenientiae modo memoratae rigidissimam exponit. Quae etsi vulgaribus principiis innititur, tamen non exiguam sagacitatem prae se ferre videtur. Quod ad ipsum argumentum attinet, id iam supra satis est explicatum.

Iam ab aliquo tempore incidi in theorema, quo natura numerorum non mediocriter illustrari est visa, cum in eo ordo contineatur, quem summae divisorum ex numeris serie naturali procedentibus ortae inter se tenent.[2]) Ostendi enim, si singulorum numerorum naturalium 1, 2, 3, 4, 5, 6, 7, 8 etc. omnes divisores in unam summam colligantur haeque divisorum summae in seriem disponantur, quae erit

$$1,\ 3,\ 4,\ 7,\ 6,\ 12,\ 8,\ 15,\ 13,\ 18,\ 12,\ 28,\ 14,\ 24,\ 24,\ 31,\ 18 \text{ etc.},$$

---

1) Hanc demonstrationem EULERUS iam in epistola d. 9. Junii 1750 ad CHR. GOLDBACH scripta exposuit, *Correspondance math. et phys. publiée par P. H. Fuss*, St.-Pétersbourg 1843, t. I, p. 515, imprimis p. 521 (vide ibidem, p. 407, EULERI epistolam d. 1. Apr. 1747 ad CHR. GOLDBACH scriptam); *LEONHARDI EULERI Opera omnia*, series III. F. R.

2) Vide Commentationes 175 et 243 huius voluminis. F. R.

hanc seriem esse recurrentem eiusque singulos terminos ex praecedentibus secundum quandam scalam relationis determinari. Atque hic ordo non solum ideo maxime notatu dignus est visus, quod vix quisquam suspicatus fuerit hanc seriem certae cuipiam legi esse adstrictam, sed etiam, quod istius ordinis nullam demonstrationem firmam mihi quidem tum temporis reperire licuerit, etiamsi pluribus modis rem tentaverim. Perductus quidem fui ad huius ordinis observationem, dum sequentem formulam in infinitum productam sum contemplatus

$$s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7) \text{ etc.},$$

ex cuius evolutione per inductionem conclusi fore[1])

$$s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + \text{etc.},$$

ubi exponentium ipsius x ordo eorum differentiis sumendis fit manifestus; erit enim series differentiarum

$$1,\ 1,\ 3,\ 2,\ 5,\ 3,\ 7,\ 4,\ 9,\ 5,\ 11,\ 6,\ 13,\ 7,\ 15,\ 8 \text{ etc.}$$

Excerptis enim terminis alternis patet hanc seriem esse permixtam ex serie numerorum imparium et ex serie numerorum omnium integrorum. Verum quod sit secundum hanc legem $s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \text{etc.}$, siquidem fuerit $s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)$ etc., per inductionem tantum collegi neque aequalitatem harum duarum formularum solida demonstratione evincere potui. Quam ob causam etiam ordinem illum, quem in summis divisorum hinc elicui, firmiter demonstrare non valui, sed eius demonstrationem iam tum inniti declaravi demonstratione aequalitatis inter binas illas formulas infinitas modo exhibitas. Cum igitur nunc istam demonstrationem sim adeptus, ordinem quoque illum in summis divisorum detectum non amplius illis veritatibus, quae agnoscuntur neque tamen demonstrari possunt, accenseri conveniet, quemadmodum tum temporis sum arbitratus, sed iam merito ipsi locus inter veritates rigide demonstratas assignari poterit. Cuius rei ne ullum dubium relinquatur, singulas propositiones, quibus demonstratio huius veritatis innititur, hic ordine apponam atque demonstrabo.

1) Vide notam p. 191. F. R.

PROPOSITIO 1

Si sit

$$s = (1+\alpha)(1+\beta)(1+\gamma)(1+\delta)(1+\varepsilon)(1+\zeta)(1+\eta) \text{ etc.,}$$

productum hoc ex infinitis factoribus constans in seriem sequentem convertitur

$$s = (1+\alpha) + \beta(1+\alpha) + \gamma(1+\alpha)(1+\beta) + \delta(1+\alpha)(1+\beta)(1+\gamma)$$
$$+ \varepsilon(1+\alpha)(1+\beta)(1+\gamma)(1+\delta) + \zeta(1+\alpha)(1+\beta)(1+\gamma)(1+\delta)(1+\varepsilon) + \text{etc.}$$

DEMONSTRATIO

Cum enim seriei primus terminus sit $(1+\alpha)$ et secundus $= \beta(1+\alpha)$, erit summa primi et secundi $= (1+\alpha)(1+\beta)$; si iam addatur tertius terminus $\gamma(1+\alpha)(1+\beta)$, prodibit $(1+\alpha)(1+\beta)(1+\gamma)$; addatur insuper terminus quartus, qui est $\delta(1+\alpha)(1+\beta)(1+\gamma)$; erit summa

$$= (1+\alpha)(1+\beta)(1+\gamma)(1+\delta).$$

Atque sic in infinitum procedendo summa totius seriei seu omnium eius terminorum perducetur ad hoc productum

$$(1+\alpha)(1+\beta)(1+\gamma)(1+\delta)(1+\varepsilon)(1+\zeta) \text{ etc.}$$

Unde manifestum est, si fuerit

$$s = (1+\alpha)(1+\beta)(1+\gamma)(1+\delta)(1+\varepsilon)(1+\zeta) \text{ etc.,}$$

fore vicissim

$$s = (1+\alpha) + \beta(1+\alpha) + \gamma(1+\alpha)(1+\beta) + \delta(1+\alpha)(1+\beta)(1+\gamma) + \text{etc.}$$

PROPOSITIO 2

Si fuerit

$$s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6) \text{ etc.,}$$

productum hoc ex infinitis factoribus constans reducetur ad hanc seriem

$$s = 1 - x - x^2(1-x) - x^3(1-x)(1-x^2) - x^4(1-x)(1-x^2)(1-x^3) - \text{etc.}$$

DEMONSTRATIO

Si haec forma $s=(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)$ etc. cum forma praecedente $s=(1+\alpha)(1+\beta)(1+\gamma)(1+\delta)(1+\varepsilon)$ etc. comparetur, manifestum est fore

$$\alpha=-x,\quad \beta=-x^2,\quad \gamma=-x^3,\quad \delta=-x^4,\quad \varepsilon=-x^5 \quad \text{etc.}$$

His igitur valoribus in serie ibi data, quae producto s aequalis est inventa, rite substitutis patebit propositionis veritas, scilicet esse

$$s=1-x-x^2(1-x)-x^3(1-x)(1-x^2)-x^4(1-x)(1-x^2)(1-x^3)-\text{etc.}$$

PROPOSITIO 3

Si fuerit

$$s=(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7)\ \text{etc.},$$

erit hoc productum infinitum per multiplicationem evolvendo terminosque secundum potestates ipsius x disponendo

$$s=1-x^1-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-x^{40}+x^{51}+x^{57}-\text{etc.},$$

cuius seriei ratio est ea ipsa, quae supra est exposita.

DEMONSTRATIO

Cum sit

$$s=(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7)\ \text{etc.},$$

erit

$$s=1-x-x^2(1-x)-x^3(1-x)(1-x^2)-x^4(1-x)(1-x^2)(1-x^3)-\text{etc.}$$

Ponatur

$$s=1-x-Ax^2;$$

erit

$$A=1-x+x(1-x)(1-x^2)+x^2(1-x)(1-x^2)(1-x^3)+\text{etc.}$$

Evolvantur singuli termini tantum secundum factorem $1-x$ ac sequenti modo disponantur

$$A=\left\{\begin{array}{l} \quad -x \qquad\qquad -x^2(1-x^2) \qquad\qquad -x^3(1-x^2)(1-x^3) \qquad\qquad -\text{etc.}\\ 1+x(1-x^2)+x^2(1-x^2)(1-x^3)+x^3(1-x^2)(1-x^3)(1-x^4)+\text{etc.}\end{array}\right.$$

eritque terminis subscriptis colligendis

$$A=1-x^3-x^5(1-x^2)-x^7(1-x^2)(1-x^3)-x^9(1-x^2)(1-x^3)(1-x^4)-\text{etc.}$$

Ponatur

$$A=1-x^3-Bx^5;$$

erit

$$B=1-x^2+x^2(1-x^2)(1-x^3)+x^4(1-x^2)(1-x^3)(1-x^4)+\text{etc.},$$

in quibus terminis singulis $1-x^2$ tantum evolvatur, ac fiet

$$B=\left\{\begin{array}{l} \quad -x^2 \qquad\qquad -x^4(1-x^3) \qquad\qquad -x^6(1-x^3)(1-x^4) \qquad\qquad -\text{etc.}\\ 1+x^2(1-x^3)+x^4(1-x^3)(1-x^4)+x^6(1-x^3)(1-x^4)(1-x^5)+\text{etc.}\end{array}\right.$$

denuoque terminis subscriptis colligendis habebitur

$$B=1-x^5-x^8(1-x^3)-x^{11}(1-x^3)(1-x^4)-x^{14}(1-x^3)(1-x^4)(1-x^5)-\text{etc.}$$

Ponatur

$$B=1-x^5-Cx^8;$$

erit

$$C=1-x^3+x^3(1-x^3)(1-x^4)+x^6(1-x^3)(1-x^4)(1-x^5)+\text{etc.},$$

ubi in singulis terminis factor $1-x^3$ evolvatur, ut fiat scribendo ut supra

$$C=\left\{\begin{array}{l} \quad -x^3 \qquad\qquad -x^6(1-x^4) \qquad\qquad -x^9(1-x^4)(1-x^5) \qquad\qquad -\text{etc.}\\ 1+x^3(1-x^4)+x^6(1-x^4)(1-x^5)+x^9(1-x^4)(1-x^5)(1-x^6)+\text{etc.},\end{array}\right.$$

unde colligetur

$$C=1-x^7-x^{11}(1-x^4)-x^{15}(1-x^4)(1-x^5)-x^{19}(1-x^4)(1-x^5)(1-x^6)-\text{etc.}$$

Ponatur

$$C=1-x^7-Dx^{11};$$

erit

$$D=1-x^4+x^4(1-x^4)(1-x^5)+x^8(1-x^4)(1-x^5)(1-x^6)+\text{etc.},$$

quae abit in hanc formam

$$D = \begin{cases} \quad - x^4 \qquad\quad - x^8(1-x^5) \qquad\quad - x^{12}(1-x^5)(1-x^6) \qquad\quad - \text{etc.} \\ 1 + x^4(1-x^5) + x^8(1-x^5)(1-x^6) + x^{12}(1-x^5)(1-x^6)(1-x^7) + \text{etc.}, \end{cases}$$

sicque erit

$$D = 1 - x^9 - x^{14}(1-x^5) - x^{19}(1-x^5)(1-x^6) - x^{24}(1-x^5)(1-x^6)(1-x^7) - \text{etc.}$$

Quodsi porro ponatur

$$D = 1 - x^9 - Ex^{14},$$

reperietur simili modo

$$E = 1 - x^{11} - Fx^{17}$$

hincque ultra

$$F = 1 - x^{13} - Gx^{20}, \quad G = 1 - x^{15} - Hx^{23}, \quad H = 1 - x^{17} - Ix^{26} \quad \text{etc.}$$

Restituamus iam successive hos valores eritque

$$\begin{aligned} s &= \quad 1 - x \quad - Ax^2, \\ Ax^2 &= x^2(1-x^3) - Bx^7, \\ Bx^7 &= x^7(1-x^5) - Cx^{15}, \\ Cx^{15} &= x^{15}(1-x^7) - Dx^{26}, \\ Dx^{26} &= x^{26}(1-x^9) - Ex^{40} \end{aligned}$$

etc.

Quamobrem habebimus

$$s = 1 - x - x^2(1-x^3) + x^7(1-x^5) - x^{15}(1-x^7) + x^{26}(1-x^9) - x^{40}(1-x^{11}) + \text{etc.}$$

sive id ipsum, quod demonstrari oportet,

$$s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + x^{51} + \text{etc.},$$

unde simul lex exponentium supra indicata per differentias luculenter perspicitur.

PROPOSITIO 4
SEU
THEOREMA PRINCIPALE DEMONSTRANDUM

Si haec scribendi formula $\int n$ *denotet summam omnium divisorum numeri n similique modo numerorum minorum, veluti* $n-\alpha$, *designentur per* $\int(n-\alpha)$, *summa divisorum numeri n seu* $\int n$ *ita pendebit a summis divisorum numerorum minorum, ut sit*

$$\int n = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \int(n-15)$$
$$- \int(n-22) - \int(n-26) + \int(n-35) + \int(n-40) - \int(n-51) - \int(n-57) + \text{etc.}$$

Ubi sequentia sunt notanda:

1. Signa $+$ et $-$ geminata terminos huius progressionis alternatim afficere.

2. Legem numerorum 1, 2, 5, 7, 12, 15, 22, 26 etc. ex eorum differentiis, quae sunt 1, 3, 2, 5, 3, 7, 4 etc., fieri manifestam; unde colligitur hos numeros omnes in formula hac generali $\frac{3xx \pm x}{2}$ contineri.

3. Quovis casu istius progressionis eos tantum terminos ab initio esse accipiendos, qui post signum $\int$ numeros affirmativos retineant; reliquos vero omnes, quibus signum $\int$ numeris negativis praefigitur, esse omittendos; ita si sit $n=10$, erit $\int 10 = \int 9 + \int 8 - \int 5 - \int 3 = 13 + 15 - 6 - 4 = 18$.

4. Quibus casibus occurrit terminus $\int(n-n)$, quod evenit, si n fuerit numerus huius seriei 1, 2, 5, 7, 12, 15 etc., iis casibus pro valore huius termini $\int(n-n)$ seu $\int 0$ assumi oportere ipsum numerum propositum n; sic si sit $n=7$, erit $\int 7 = \int 6 + \int 5 - \int 2 - \int 0 = 12 + 6 - 3 - 7 = 8$, et si sit $n = 12$, erit $\int 12 = \int 11 + \int 10 - \int 7 - \int 5 + \int 0 = 12 + 18 - 8 - 6 + 12 = 28$.

DEMONSTRATIO

Formetur series

$$z = x\int 1 + x^2\int 2 + x^3\int 3 + x^4\int 4 + x^5\int 5 + \text{etc.},$$

ubi quaelibet potestas ipsius x multiplicata sit per summam divisorum exponentis eius potestatis. Quodsi iam singulae divisorum summae resolvantur, manifestum est hanc seriem transformari in hanc formam

$$\begin{aligned} z = 1(x + x^2 + x^3 + x^4 + x^5 + \text{etc.}) + 2(x^2 + x^4 + x^6 + x^8 + x^{10} + \text{etc.}) \\ + 3(x^3 + x^6 + x^9 + x^{12} + x^{15} + \text{etc.}) + 4(x^4 + x^8 + x^{12} + x^{16} + x^{20} + \text{etc.}) \\ + 5(x^5 + x^{10} + x^{15} + x^{20} + x^{25} + \text{etc.}) + 6(x^6 + x^{12} + x^{18} + x^{24} + x^{30} + \text{etc.}) \\ \text{etc.}, \end{aligned}$$

quibus seriebus geometricis summatis fiet

$$z = \frac{1x}{1-x} + \frac{2xx}{1-xx} + \frac{3x^3}{1-x^3} + \frac{4x^4}{1-x^4} + \frac{5x^5}{1-x^5} + \frac{6x^6}{1-x^6} + \text{etc.}$$

Multiplicetur haec forma per $-\frac{dx}{x}$ ac producti integrale erit

$$-\int \frac{z\,dx}{x} = l(1-x) + l(1-xx) + l(1-x^3) + l(1-x^4) + l(1-x^5) + \text{etc.}$$

seu

$$-\int \frac{z\,dx}{x} = l(1-x)(1-xx)(1-x^3)(1-x^4)(1-x^5)(1-x^6)\ \text{etc.};$$

quae expressio post signum logarithmicum cum sit eadem, quae in propositione praecedente vocata est $= s$, erit $-\int \frac{z\,dx}{x} = ls$ ideoque alterum valorem pro s sumendo erit quoque

$$-\int \frac{z\,dx}{x} = l(1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.}),$$

cuius differentiale per $\frac{-dx}{x}$ divisum dabit alium valorem pro z, nempe

$$z = \frac{1x + 2x^2 - 5x^5 - 7x^7 + 12x^{12} + 15x^{15} - 22x^{22} - \text{etc.}}{1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + \text{etc.}};$$

qui valor si aequalis ponatur assumto et utrinque per denominatorem $1 - x - x^2 + x^5 + x^7 - x^{12}$ etc. multiplicetur, reperietur terminis secundum potestates ipsius x disponendis omnibusque ad eandem partem collocandis:

$$\begin{array}{rlllllllllll}
0 = & x\int 1 + & x^2\int 2 + & x^3\int 3 + & x^4\int 4 + & x^5\int 5 + & x^6\int 6 + & x^7\int 7 + & x^8\int 8 + & x^9\int 9 + & x^{10}\int 10 + \text{etc.} \\
 & & -\int 1 - & \int 2 - & \int 3 - & \int 4 - & \int 5 - & \int 6 - & \int 7 - & \int 8 - & \int 9 \\
 & & & -\int 1 - & \int 2 - & \int 3 - & \int 4 - & \int 5 - & \int 6 - & \int 7 - & \int 8 \\
 & & & & & & +\int 1 + & \int 2 + & \int 3 + & \int 4 + & \int 5 \\
 & & & & & & & & +\int 1 + & \int 2 + & \int 3 \\
 & & & & & & & & & & \vdots \\
 & -1 - & 2 & * & * + & 5 & * + & 7 & * & * & *
\end{array}$$

Unde singularum potestatum ipsius x coefficientibus nihilo aequatis sequitur fore

$$\begin{array}{ll}
\int 1 = 1, & \int 6 = \int 5 + \int 4 - \int 1, \\
\int 2 = \int 1 + 2, & \int 7 = \int 6 + \int 5 - \int 2 - 7, \\
\int 3 = \int 2 + \int 1, & \int 8 = \int 7 + \int 6 - \int 3 - \int 1, \\
\int 4 = \int 3 + \int 2, & \int 9 = \int 8 + \int 7 - \int 4 - \int 2, \\
\int 5 = \int 4 + \int 3 - 5, & \int 10 = \int 9 + \int 8 - \int 5 - \int 3;
\end{array}$$

atque indolem illius aequationis vel leviter attendenti patebit esse generatim

$$\int n = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \int(n-15) - \text{etc.}$$

hac progressione quovis casu eousque continuata, donec perveniatur ad summas numerorum negativorum. Deinde per se est perspicuum numeros absolutos 1, 2, 5, 7 etc., qui in illis formulis conspiciuntur, vicem tenere termini $\int 0$; unde concluditur in casibus, quibus pro $\int n$ in progressione illa reperta occurrit terminus $\int(n-n)$ seu $\int 0$, valorem eius semper ipsi numero proposito n aequalem esse capiendum; sicque habetur plena ac perfecta demonstratio theorematis propositi, quae, cum praeter tractationem serierum infinitarum per logarithmos et differentialia procedat, minus quidem naturalis, sed ob hoc ipsum multo magis notabilis est aestimanda.

DE PROBLEMATIBUS INDETERMINATIS QUAE VIDENTUR PLUS QUAM DETERMINATA[1]

Commentatio 253 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 6 (1756/7), 1761, p. 85—114
Summarium ibidem p. 12—14

SUMMARIUM

Argumentum huius dissertationis omnino est novum atque insignem promotionem Analyseos indeterminatae, quae vulgo methodus DIOPHANTEA appellari solet, polliceri videtur, siquidem summi EULERI vestigia premendo omni studio uberius excolatur. Primum autem accuratius hic definitam cernimus indolem problematum indeterminatorum, qualia quidem DIOPHANTUS pertractavit, quae vulgo perperam innumerabiles solutiones admittere videntur. Natura scilicet cuiusque quaestionis ex sua ipsius indole potius quam ex solutione, quae initio nondum constat, diiudicari debet. Ita dantur quaestiones nullam plane solutionem admittentes, quae tamen nihilominus ad indeterminatas sunt referendae; veluti si quaerantur duo cubi, quorum summa sit cubus, vel quatuor quadrata in arithmetica progressione. Postquam enim diu multumque in his solvendis fuerit elaboratum, tum demum agnoscimus nullam solutionem dari, quod autem non impedit, quominus istiusmodi quaestiones pro indeterminatis habeantur. Simili modo dantur etiam eiusmodi quaestiones indeterminatae, quae plures una solutiones non admittunt, veluti si quaeratur cubus, qui unitate auctus efficiat quadratum. Melius ergo problemata indeterminata ita definiuntur, ut dicantur circa numeros rationales tantum ac saepenumero integros tantum versari. Ita si quaeri debeant duo biquadrata, quorum summa faciat quadratum, quaestio omnino est huius generis, cum radix quadrata ex summa biquadratorum debeat esse numerus ratio-

1) Cf. quoque L. EULER, *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, Zweyter Theil, zweyter Abschnitt, Cap. 14; *LEONHARDI EULERI Opera omnia*, series I, vol. 1. F. R.

nalis, etiamsi solutio ipsa sit impossibilis. Saepenumero plures conditiones simul proponi solent, veluti si quaerantur tres eiusmodi numeri, ut binorum productum, si tertio addatur, faciat quadratum, ubi utique tribus conditionibus est satisfaciendum; hocque adeo infinitis modis praestari potest. Sin autem insuper nova conditio adiiciatur, sine dubio numerus solutionum restringetur atque adeo interdum fit impossibilis. Veluti si quaerantur duo quadrata, quorum summa sit quadratum, id utique infinitis modis fieri potest; at adiecta insuper hac conditione, ut etiam eorundem quadratorum differentia sit quadratum, quaestio subito fit impossibilis. Ita pleraque problemata, quae DIOPHANTUS tractavit, ita sunt comparata, ut nova adiecta conditione fiant impossibilia, hocque casu plus quam determinata vocari solent.

Nunc igitur Cel. Auctor ostendit infinita dari huiusmodi problemata, quibus etsi adiiciantur non una, sed plures novae conditiones, solutionum tamen numerus revera maneat infinitus. Neque vero putandum est tales conditiones pro lubitu adiici posse, sed eas certo modo ad ipsam quaestionis indolem adstrictas esse oportet, alioquin certo plus quam determinata essent evasura. Ita in quaestione memorata de tribus numeris, ut binorum productum tertio additum faciat quadratum, insuper hae conditiones adiici possunt, ut binorum productum summae eorundem binorum additum faciat quadratum, quae tres novae conditiones adiectae non impediunt, quominus adhuc innumerabiles solutiones locum habeant. Si praeterea postuletur, ut etiam summa productorum ex binis fiat quadratum, quaestio adhuc infinitas solutiones admittit neque solutionum numerus minuitur, si insuper summa ipsorum numerorum summae productorum ex binis adiecta quadratum efficere debeat; quin etiam Auctor ostendit plures adhuc conditiones adiici posse manente solutionum numero infinito.

Tales quaestiones, nisi conditiones certa lege inter se essent connexae, quae connexio autem in ipsa propositione non perspicitur, merito tanquam plus quam determinatae reiiciendae videntur ac temere quisquam earum solutionem susciperet, antequam probe perspexerit, simulatque aliquibus certo modo satisfecerit, reliquis omnibus sponte satisfieri. In DIOPHANTO adeo iam eiusmodi quaestiones reperiuntur, quarum solutionem ex certis porismatibus derivavit, quorum vim commentatores minus agnoverunt. Hoc ergo argumentum sollicite hic evolvitur ac non solum porismata, quibus DIOPHANTUS est usus, dilucide explicantur et ex simplicissimis principiis deducuntur, sed etiam indidem multo abstrusiora eliciuntur, quorum beneficio innumerabiles quaestiones, quae alioquin omnes Analyseos vires superare videantur, facili negotio resolvi queunt.

Omnia problemata, quae in Analysi DIOPHANTEA proponi solent, esse indeterminata vel ipsa rei natura declarat; etsi enim plures eiusmodi quaestiones occurrant, quae nonnisi unicam solutionem admittunt, veluti si quaeratur cubus, qui unitate auctus faciat quadratum, cui quaestioni praeter cubum 8 alius nullus satisfacere reperitur, tamen ne tales quidem quaestiones ad problemata determinata referri convenit, propterea quod methodus eas resolvendi tota ex ratione problematum indeterminatorum est petita atque casui potissimum singulari tribuendum videtur, si unica solutio tantum locum habeat. Quemadmodum etiam non desunt eiusmodi quaestiones, quae plane nullam solutionem admittunt, quae tamen nihilominus quaestionibus indeterminatis recte annumerantur; ante enim quam certiores fuerimus facti nullam dari solutionem, id quod operatio ususque methodorum demum declarat, eas pro indeterminatis omnino habere debemus nostramque investigationem perinde adornare, ac si infinita solutionum multitudo daretur. Ita si quaeri debeant tria quadrata, quorum summa faciat septem, nemo dubitabit, quin haec quaestio indeterminatis sit accensenda, etiamsi deinceps investigatione peracta impossibilitas solutionis manifesto se prodat.

Quando igitur hic de problematibus indeterminatis tractare constitui, quae plus quam determinata videantur, ne quis putet haec invicem pugnare fierique non posse, ut, quod indeterminatum sit, idem plus quam determinatum videri queat, instituti rationem clarius exponi oportere sentio. Ac primo quidem nullum est dubium, quin cuilibet quaestioni DIOPHANTEAE eiusmodi insuper conditiones adiici queant, quibus ea non tam determinata quam impossibilis reddatur. Veluti si quaestioni, qua duo quadrata petuntur, quorum summa sit quadratum, insuper haec conditio adiiciatur, ut eorundem quadratorum differentia quoque sit quadratum, quaestio, quae primum erat maxime indeterminata, hac unica conditione adiuncta fit impossibilis ideoque merito pro plus quam determinata habetur. Simili modo tria quadrata quaerere in progressione arithmetica problema est indeterminatum et innumerabiles solutiones admittens; statim vero ac quatuor quadrata in arithmetica progressione requiruntur, problema non determinatur, sed prorsus fit impossibile et plus quam determinatum.

Ex his exemplis manifestum est quaestionem indeterminatam per additionem unicae conditionis reddi posse plus quam determinatam ideoque impossibilem. E contrario vero dantur eiusmodi quoque quaestiones, quae iam

tot conditiones continent, ut unica nova conditione super addita pari iure ac commemoratae plus quam determinatae fieri debere videantur, quibus tamen nihilominus non una, sed plures saepe conditiones adiungi possunt, ita ut iis non obstantibus infinitae adhuc solutiones exhiberi queant; cuiusmodi casus ex hoc problemate clarissime intelligetur:

Quaerantur tres numeri, ut binorum productum addito tertio fiat quadratum.[1])

Scilicet vocando hos tres numeros x, y, z requiritur, ut sit

$$xy + z = \text{quadrato}, \quad xz + y = \text{quadrato}, \quad yz + x = \text{quadrato}.$$

Haec quaestio tentanti, nisi singularia artificia adhibeantur, iam solutu tam difficilis apparebit, ut, si nova conditio super adderetur, de solutione plane sit desperaturus. Si enim ponat $xy + z = aa$, ut habeat $z = aa - xy$, ambae reliquae formulae quadratum efficiendae erunt

$$aax - xxy + y \quad \text{et} \quad aay - xyy + x;$$

quarum priorem si ponat $= bb$, habebit quidem $y = \frac{aax - bb}{xx - 1}$; at hoc valore in tertia substituto quadratum reddi debebit haec expressio

$$x^5 - 2x^3 + aabbxx - (a^4 + b^4 - 1)x + aabb,$$

quae certe iam est tam complicata, ut omnem solutoris sollertiam requirat neque de novis conditionibus insuper adimplendis sit cogitandum.

Interim tamen huic quaestioni has insuper conditiones adiicere licet, ut binorum numerorum productum cum eorundem summa quoque faciat quadratum seu ut sit

$$xy + x + y = \square, \quad xz + x + z = \square, \quad yz + y + z = \square.\text{[2])}$$

Quis igitur non putaret his tribus conditionibus adiectis problema propositum iam per se satis difficile fieri plus quam determinatum? Interim tamen certum est et hoc casu problema adhuc esse indeterminatum atque adeo in numeris integris infinitas solutiones admittere.

1) Cf. quaestionem XII libri III DIOPHANTI *Arithmeticorum* (ed. TANNERY; quae quaestio est quaestio XIV editionis BACHETI); vide notam p. 404 huius voluminis. F. R.

2) Cf. quaestionem XV libri III DIOPHANTI *Arithmeticorum* (ed. TANNERY; quae quaestio est quaestio XVII editionis BACHETI); vide notam p. 404 huius voluminis. Vide etiam FERMATII observationem ad hanc quaestionem (cf. notam 2 p. 51 huius voluminis), *Oeuvres de FERMAT*, t. I, p. 292. F. R.

Quin etiam insuper hae conditiones adiici possunt manente solutionum numero et quidem in numeris integris infinito: 1⁰. ut summa productorum ex binis sit quadratum, 2⁰. ut eadem summa productorum ex binis una cum ipsorum numerorum summa fiat quadratum.

Nec vero nunc quidem conditionum multitudo exhausta est censenda; nam postulari insuper potest, ut trium quaesitorum numerorum vel unus vel adeo duo sint ipsi quadrati, et quidem integri. Quodsi autem omnes tres debeant esse quadrati, ne nunc quidem problema fit plus quam determinatum, sed infinitas adhuc solutiones, etsi non in numeris integris, admittit; ac fortasse adhuc plures conditiones addi possent, quibus quoque satisfieri liceret.

En ergo problema, quod merito cuique plus quam determinatum videri debet:

Invenire tres numeros integros x, y, z, ut sequentes formulae omnes fiant quadrata

$$xy + z = \square, \quad xz + y = \square, \quad yz + x = \square,$$

$$xy + x + y = \square, \quad xz + x + z = \square, \quad yz + y + z = \square,$$

$$xy + xz + yz = \square,$$

$$xy + xz + yz + x + y + z = \square,$$

cuius simplicissima solutio sine dubio est

$$x = 1, \quad y = 4 \quad \text{et} \quad z = 12;$$

tum vero etiam sequentes solutiones in promptu sunt

$$\begin{aligned} x &= 1, & y &= 12, & z &= 24, \\ x &= 4, & y &= 9, & z &= 28, \\ x &= 4, & y &= 12, & z &= 33, \\ x &= 1, & y &= 24, & z &= 40, \\ x &= 1, & y &= 40, & z &= 60, \\ x &= 4, & y &= 33, & z &= 64. \end{aligned}$$

Verum si haec conditio insuper sit adiecta, ut ipsi tres numeri quaesiti debeant esse quadrati, in fractis ecce has solutiones

$$x = \frac{9}{64}, \quad y = \frac{25}{64}, \quad z = \frac{49}{16},$$

$$x = \frac{49}{64}, \quad y = \frac{225}{64}, \quad z = \frac{169}{16},$$

$$x = \frac{25}{9}, \quad y = \frac{64}{9}, \quad z = \frac{196}{9},$$

$$x = \frac{9}{25}, \quad y = \frac{64}{25}, \quad z = \frac{196}{25}.$$

Huiusmodi autem quaestio, inquam, merito pro plus quam determinata habetur; has enim conditiones non pro arbitrio adiecimus atque in ipsa indagatione huiusmodi conditionum, quas indoles problematis patitur, praecipua pars artificii continetur. Namque si quis ad arbitrium conditiones superaddere vellet, admodum probabile esset problema vel unica adiecta revera fieri plus quam determinatum; quamobrem talia problemata tot conditionibus onerata recte statim tanquam plus quam determinata spectantur, nisi aliunde constet conditiones eas ab insigni artificio esse adiectas.

Talia problemata autem iam in ipso DIOPHANTO occurrunt, quae commentatoribus non parum negotii fecerunt, cum quaedam tantum conditiones calculum tantopere occupent, ut reliquarum ratio neutiquam haberi posse videatur. Praemittuntur autem eiusmodi problematibus certae quaedam propositiones, quae ibi *Porismata*[1]) vocantur, in quibus tota solutionis vis con-

1) Vide de his porismatis quaestiones III, V, XVI libri V DIOPHANTI *Arithmeticorum* (ed. TANNERY; quae quaestiones sunt quaestiones III, V, XIX editionis BACHETI): *Diophanti Alexandrini Arithmeticorum libri sex et de numeris multangulis liber unus.* Nunc primum graece et latine editi, atque absolutissimis commentariis illustrati. Auctore C. G. BACHETO, Lutetiae Parisiorum 1621, p. 288, 289, 290, 291, 322—324; *Die Arithmetik und die Schrift über Polygonalzahlen des Diophantus von Alexandria.* Übersetzt und mit Anmerkungen begleitet von G. WERTHEIM, Leipzig 1890, p. 195, 198, 226 (qua in editione etiam FERMATII observationes ad DIOPHANTUM BACHETI continentur; cf. notam 2 p. 51); *Diophanti Alexandrini opera omnia cum graecis commentariis.* Edidit et latine interpretatus est P. TANNERY, vol. I, Lipsiae 1893, p. 316, 317, 320, 321, 358, 359, vol. II, Lipsiae 1895, p. XIX (respiciendum est hac in editione *Arithmeticorum* quaestiones aliter numeratas esse atque in editione BACHETI).

Vide etiam M. CANTOR, *Vorlesungen über Geschichte der Mathematik*, Bd. 1, 3. Aufl., Leipzig 1907, p. 467 et 483, praecipue autem G. H. F. NESSELMANN, *Die Algebra der Griechen*, Berlin 1842, p. 269—272, 437—461, H. HANKEL, *Zur Geschichte der Mathematik in Alterthum und Mittelalter*, Leipzig 1874, p. 168—171, T. L. HEATH, *Diophantus of Alexandria. A study in the history of greek algebra.* Second edition. With a supplement containing an account of FERMAT's theorems and problems connected with DIOPHANTINE analysis and some solutions of DIOPHANTINE problems by EULER, Cambridge 1910, p. 99—110. F. R.

tinetur. Ostenditur scilicet, si quibusdam conditionibus certo quodam modo satisfiat, tum simul aliis quoque conditionibus quasi sponte satisfieri, ita ut non opus sit calculum seorsim ad eas applicare. Ita pro quaestione exempli loco allegata, qua tres numeri x, y et z quaeruntur, ut conditiones praescriptae impleantur, porisma praemittendum ita se habet:

Si quaerantur duo numeri x et y, ut $xy+x+y$ fiat quadratum, puta $=uu$, atque tertius numerus z ita capiatur, ut sit $z=1+x+y\pm 2u$, tum non solum hae formulae

$$xz+x+z \quad \text{et} \quad yz+y+z$$

fient quadrata, sed etiam hae

$$xy+z, \quad xz+y \quad \text{et} \quad yz+x$$

una cum istis

$$xy+xz+yz$$

et

$$xy+xz+yz+x+y+z$$

sponte fient quadrata.

Cum igitur huic unicae conditioni, qua formula $xy+x+y$ quadratum reddi debet, facillime satisfiat, ope huius porismatis quaestio tam multis conditionibus circumscripta, ut plus quam determinata videatur, nullo plane labore infinitis modis resolvitur et quidem in numeris integris. Ponatur enim

$$xy+x+y=uu,$$

et cum sit

$$xy+x+y+1=(x+1)(y+1)=uu+1,$$

pro uu tale sumatur quadratum, quod unitate auctum habeat factores; sit scilicet $uu+1=mn$ et numeri problemati satisfacientes erunt

$$x=m-1, \quad y=n-1 \quad \text{et} \quad z=m+n-1\pm 2u.$$

In huiusmodi igitur problematibus totum negotium vertitur in inventione idoneorum illorum porismatum, quibus tota solutio ita contineatur, ut, statim atque aliquibus conditionibus satisfecerimus, simul reliquas adimpleverimus. Cum igitur ratio talium porismatum a nemine adhuc sit explicata, si eam accuratius exposuero, non exiguum incrementum universa Analysis DIOPHANTEA inde accepisse erit existimanda. Tota autem horum porismatum ratio sequenti lemmati per se perspicuo inniti videtur.

LEMMA

1. *Si inventi fuerint valores litterarum z, y, x etc., quibus aequationi $W=0$ satisfiat existente W functione quacunque illarum litterarum z, y, x etc., atque P, Q, R etc. eiusmodi fuerint quantitates, ut $P+W$, $Q+W$, $R+W$ etc. fiant quadrata, tum iisdem valoribus pro z, y, x etc. assumtis fient quoque quantitates P, Q, R etc. quadrata.*

Ratio huius lemmatis est manifesta, quia pro litteris z, y, x etc. tales valores assumi ponuntur, ut fiat $W=0$; ideoque si $P+W$, $Q+W$, $R+W$ sint quadrata, etiam quantitates P, Q, R ipsae quadrata sint necesse est.

COROLLARIUM 1

2. Formulae quoque P, Q, R etc. reddentur quadrata, si fuerint $P+\alpha W$, $Q+\beta W$, $R+\gamma W$ etc. quadrata, vel etiam generalius si istae expressiones

$$P+\alpha W+\zeta W^2, \quad Q+\beta W+\eta W^2, \quad R+\gamma W+\theta W^2$$

fuerint quadrata.

COROLLARIUM 2

3. Vicissim ergo etiam si litteris z, y, x etc. tales assignati fuerint valores, ut fiat $W=0$, tum etiam omnes huius generis formulae $PP+\alpha W$, $QQ+\beta W$, $RR+\gamma W$ etc. fient quadrata.

COROLLARIUM 3

4. Quodsi ergo aequationi $W=0$ infinitis diversis modis satisfieri queat, tum iisdem modis omnes huius generis formulae $PP+\alpha W$, $QQ+\beta W$, $RR+\gamma W$ etc. quadrata efficientur.

COROLLARIUM 4

5. Cum igitur numerus huiusmodi formularum in infinitum augeri possit, manifestum est, quomodo etiam infinitae conditiones praescribi possint, quibus omnibus satisfiat, simulatque unicae conditioni, scilicet aequationi $W=0$, fuerit satisfactum.

COROLLARIUM 5

6. Simili modo hoc lemma ad cubos aliasve potestates altiores quascunque extendetur. Si enim factum fuerit $W=0$, tum quoque omnes huiusmodi formulae $P^3+\alpha W$ fient cubi et hae $P^4+\alpha W$ biquadrata, et ita porro, quaecunque etiam quantitates pro P accipiantur.

SCHOLION 1

7. Ratio quidem huius lemmatis tam est obvia, ut id nihil in recessu habere videatur; si enim P, Q, R etc. cum W fuerint functiones quaecunque litterarum z, y, x etc. harumque valores quaerantur, quibus sequentes formulae

$$PP+\alpha W, \quad QQ+\beta W, \quad RR+\gamma W \text{ etc.}$$

fiant quadrata, statim utique in oculos incurrit his omnibus conditionibus satisfieri, dummodo haec una $W=0$ adimpleatur; verum plerumque ratio talis compositionis in formulis propositis tam est occulta, ut difficillimum sit eam quantitatem W assignare, qua deleta partes residuae formularum sponte fiant quadrata. Quin etiam non adeo foret difficile hanc compositionem ita abscondere, ut eius investigatio iam per se arduum problema constitueret. Vicissim autem data aequatione $W=0$ operam haud inutiliter collocari arbitror, si formulae simpliciores investigentur, quae tum in quadrata abibunt; hoc enim modo plurima insignia et concinna reperientur problemata, quorum solutio erit in promtu, cuiusmodi est id, cuius supra mentio est facta. Hunc in finem aequationem $W=0$ talem assumi conveniet, ut litterae z, y, x etc. in eam aequaliter ingrediantur atque inter se permutari patiantur; tum enim si PP eiusmodi fuerit quadratum, ut sit $PP+\alpha W$ quadratum, permutandis litteris z, y, x etc. in PP, unde prodeant QQ, RR etc., etiam $QQ+\beta W$ et $RR+\gamma W$ fient quadrata.

SCHOLION 2

8. Duplex ergo hinc nascitur tractationis nostrae partitio; primam scilicet constituet litterarum z, y, x etc., circa quas quaestio versatur, numerus, prouti duo vel tres vel plures quaeruntur numeri, qui datis conditionibus sint praediti. Alteram partitionem suppeditabit dimensionum numerus, ad quem litterae z, y, x etc. in aequatione $W=0$ assurgunt; quae aequatio cum ita debeat esse comparata, ut resolutionem admittat, nullius quantitatum

altior potestas quam secunda occurrere debet, quia alioquin resolutio in numeris rationalibus absolvi non posset. Quare generalis forma aequationis $W=0$, quam hic tractabimus, erit

$$\begin{gathered}0=\alpha+\beta(z+y+x+\text{etc.})\\+\gamma(zy+zx+yx+\text{etc.})+\delta(zz+yy+xx+\text{etc.})\\+\varepsilon(zzy+zyy+zzx+zxx+\text{etc.})+\zeta(zyx+\text{etc.})\\+\eta(zzyy+zzxx+yyxx+\text{etc.})+\theta(zzyx+zyyx+\text{etc.})\\\text{etc.},\end{gathered}$$

quandoquidem numeri z, y, x etc. in ea debent esse permutabiles. Secundum hanc duplicem ergo partitionem sequentia problemata contemplemur ab iis inchoaturi, in quibus duo numeri z et y quaerendi proponuntur.

PROBLEMA 1

9. *Proposita hac aequatione resolvenda*

$$\alpha=\beta(z+y)$$

invenire formulas simpliciores, quae per eius resolutionem redduntur quadrata.

SOLUTIO

Cum huic aequationi $\alpha=\beta(z+y)$ fuerit satisfactum, manifestum est simul hanc formam generalem

$$PP+M(-\alpha+\beta(y+z))$$

fieri quadratum, quaecunque quantitates pro P et M accipiantur. Quia β evanescere nequit, ponamus $\beta=1$, ut inter y et z haec subsistat relatio $y+z=a$ sitque

$$PP+M(y+z-a)=\text{quadrato},$$

unde sequentes casus notatu dignos evolvamus.

I. Sit $M=2$; erit

$$PP+2y+2z-2a=\text{quadrato}.$$

Capiatur $P = y - 1$; erit

$$1)\quad yy + 2z + 1 - 2a = \square$$

et permutatione facta

$$2)\quad zz + 2y + 1 - 2a = \square.$$

Capiatur $P = y + z - 1$; erit

$$3)\quad (y + z)^2 + 1 - 2a = \square.$$

Capiatur $P = y - z + 1$; erit

$$4)\quad (y - z)^2 + 4y + 1 - 2a = \square,$$

$$5)\quad (y - z)^2 + 4z + 1 - 2a = \square.$$

II. Sit $M = -2$, unde

$$PP - 2y - 2z + 2a = \text{quadrato}.$$

Capiatur $P = y + 1$ seu $P = z + 1$; erit

$$6)\quad yy - 2z + 1 + 2a = \square,$$

$$7)\quad zz - 2y + 1 + 2a = \square.$$

Capiatur $P = y + z + 1$; erit

$$8)\quad (y + z)^2 + 1 + 2a = \square.$$

Capiatur $P = y - z + 1$; erit

$$9)\quad (y - z)^2 - 4z + 1 + 2a = \square,$$

$$10)\quad (y - z)^2 - 4y + 1 + 2a = \square.$$

III. Sit $M = 2n$, unde

$$PP + 2ny + 2nz - 2na = \text{quadrato},$$

atque non solum formulae praecedentes, sed infinitae aliae orientur.

Capiatur $P = y - n$ et $P = z - n$; erit

$$11)\quad yy + 2nz + nn - 2na = \square,$$

$$12)\quad zz + 2ny + nn - 2na = \square.$$

Capiatur $P = y - 2n$ et $P = z - 2n$; erit

$$13)\quad yy - 2ny + 2nz + 4nn - 2na = \square,$$

$$14)\quad zz - 2nz + 2ny + 4nn - 2na = \square.$$

Capiatur $P = y + z - n$; erit

15) $(y+z)^2 + nn - 2na = \square$.

Capiatur $P = y + z - 2n$; erit

16) $(y+z)^2 - 2n(y+z) + 4nn - 2na = \square$.

Capiatur $P = y - z - n$; erit

17) $(y-z)^2 + 4nz + nn - 2na = \square$,

18) $(y-z)^2 + 4ny + nn - 2na = \square$.

IV. Sit $M = -y$, unde

$$PP - yy - yz + ay = \text{quadrato}.$$

Capiatur $P = y$; erit

19) $-yz + ay = \square$,

20) $-yz + az = \square$.

Capiatur $P = y - \frac{1}{2}a$; erit

21) $-yz + \frac{1}{4}aa = \square$.

Capiatur $P = y + z$; erit

22) $zz + yz + ay = \square$,

23) $yy + yz + az = \square$.

Capiatur $P = y + z - \frac{1}{4}a$; erit

24) $zz + yz + \frac{1}{2}ay - \frac{1}{2}az + \frac{1}{16}aa = \square$,

25) $yy + yz + \frac{1}{2}az - \frac{1}{2}ay + \frac{1}{16}aa = \square$.

V. Sit $M = -z - y$, unde

$$PP - (y+z)^2 + a(y+z) = \text{quadrato}.$$

Capiatur $P = y + z$; erit

26) $ay + az = \square$.

Capiatur $P = y + z - a$; erit

27) $aa - ay - az = \square$.

Capiatur $P = y - z$; erit

28) $-4yz + a(y+z) = \square.$

Capiatur $P = y - z - \frac{1}{2}a$; erit

29) $-4yz + 2az + \frac{1}{4}aa = \square,$

30) $-4yz + 2ay + \frac{1}{4}aa = \square.$

Capiatur $P = y - \frac{1}{2}a$; erit

31) $-zz - 2yz + az + \frac{1}{4}aa = \square,$

32) $-yy - 2yz + ay + \frac{1}{4}aa = \square.$

VI. Sit $M = (y + z + a)$, unde

$$PP + (y+z)^2 - aa = \text{quadrato}.$$

Capiatur $P = yz - 1$; erit

33) $yyzz + yy + zz + 1 - aa = \square.$

VII. Sit $M = n(y + z + a)$, unde

$$PP + n(y+z)^2 - naa = \text{quadrato}.$$

Capiatur $P = yz - n$; erit

34) $yyzz + nyy + nzz + nn - naa = \square.$

VIII. Sit $M = (y + z + a)(y - z + a)(z - y + a)$, unde fit

$$PP - y^4 - z^4 - a^4 + 2yyzz + 2aayy + 2aazz = \text{quadrato}.$$

Capiatur $P = yy - zz$; erit

35) $2yy + 2zz - aa = \square.$

Capiatur $P = yy + zz + aa$; erit

36) $yyzz + aayy + aazz = \square.$

IX. Sit $M = 3(y + z + a)(y - z + a)(z - y + a)$, unde fit

$$PP - 3y^4 - 3z^4 - 3a^4 + 6yyzz + 6aayy + 6aazz = \text{quadrato}.$$

Capiatur $P = 2yy + 2zz + 2aa$; erit

37) $y^4 + z^4 + 14yyzz + 14aayy + 14aazz + a^4 = \square$.

Capiatur $P = 2yy + 2zz - 2aa$; erit

38) $y^4 + z^4 + a^4 + 14yyzz - 2aayy - 2aazz = \square$,

39) $y^4 + z^4 + a^4 - 2yyzz + 14aayy - 2aazz = \square$,

40) $y^4 + z^4 + a^4 - 2yyzz - 2aayy + 14aazz = \square$.

X. Sit generalius $M = (nn-1)(y+z+a)(y-z+a)(z-y+a)$, unde fit

$$PP - (nn-1)(y^4 + z^4 + a^4 - 2yyzz - 2aayy - 2aazz) = \text{quadrato}.$$

Capiatur $P = n(yy + zz + aa)$; erit

41) $y^4 + z^4 + a^4 + 2(2nn-1)(yyzz + aayy + aazz) = \square$.

Capiatur $P = n(yy + zz - aa)$; erit

42) $y^4 + z^4 + a^4 + 2(2nn-1)yyzz - 2aayy - 2aazz = \square$,

43) $y^4 + z^4 + a^4 - 2yyzz + 2(2nn-1)aayy - 2aazz = \square$,

44) $y^4 + z^4 + a^4 - 2yyzz - 2aayy + 2(2nn-1)aazz = \square$.

COROLLARIUM 1

10. Ex his satis intelligitur infinitas exhiberi posse formulas, quae omnes per eandem relationem aequatione $y + z = a$ contentam in numeros quadratos abeant. Quotcunque ergo formulae proponantur ad quadrata reducendae, dummodo illae in his erutis contineantur, omnibus simul satisfiet ponendo $y + z = a$.

COROLLARIUM 2

11. Ita si a sit $= 1$, sequentibus formulis omnibus

$$yy + 4z = \square,\ yy - y + z = \square,\ y + z = \square,\ y - yz = \square,\ zz + 4y = \square,$$

$$zz - z + y = \square,\ (y+z)^2 - 1 = \square,\ z - yz = \square,\ yyzz + yy + zz = \square,$$

$$2yy + 2zz - 1 = \square$$

satisfit ponendo $y + z = 1$ seu $y = 1 - z$.

COROLLARIUM 3

12. Imprimis hic notanda est forma

$$yyzz + yy + zz,$$

quae in quadratum transit, si capiatur $y = 1 - z$ vel magis generaliter $y = \pm 1 \pm z$. Solutio haec apud DIOPHANTUM frequentissime[1]) occurrit, cuius fundamentum in porismate quodam constituit, pluraque affert problemata, quae eius beneficio resolvuntur.

COROLLARIUM 4

13. Simili modo haec forma latius patens

$$yyzz + aayy + aazz$$

redditur quadratum ponendo $y = \pm a \pm z$. Atque haec eadem positio facit etiam hanc formam

$$yyzz + nyy + nzz + nn - naa$$

quadratum, quicunque numerus pro n assumatur. Unde si $a = 1$, haec forma

$$yyzz + nyy + nzz + nn - n$$

sive haec

$$(yy + n)(zz + n) - n$$

fit quadratum ponendo $z = y \pm 1$. Quod etiam est insigne porisma DIOPHANTI.

SCHOLION

14. Omni attentione utique dignum est, quod tam levi opera pluribus conditionibus simul satisfieri possit, cum quaelibet conditio peculiarem operationem exigere videatur. Quin etiam hic eiusmodi formulae occurrunt, quae, si solae proponerentur, per methodos consuetas nonnisi difficulter resolvi possent, cuiusmodi est haec [formula 37]

$$y^4 + z^4 + a^4 + 14yyzz + 14aayy + 14aazz = \text{quadrato},$$

1) Cf. exempli gratia quaestionem XV libri III et quaestiones III—V libri V DIOPHANTI *Arithmeticorum* (ed. TANNERY); vide notas p. 402 et 404 huius voluminis. F. R.

cuius solutio, si more consueto tentetur, non exiguis difficultatibus implicata deprehenditur; ex quo, si praeterea aliae conditiones praescribantur, quibus simul satisfieri oporteat, quaestio non immerito plus quam determinata ac vires Analyseos transcendens videri debet. Continetur ergo in evolutione huius problematis iam porisma amplissimum, quod in Analysi DIOPHANTEA summum habet usum; quod cum natum sit ex positione simplicissima $z+y=a$, ita formulae magis compositae nos ad profundiora ac magis recondita porismata manuducent.

PROBLEMA 2

15. *Proposita hac aequatione resolvenda*

$$yz-a(y+z)+b=0$$

invenire formulas notabiliores, quae per eius resolutionem redduntur quadrata.

SOLUTIO

Sumta relatione inter numeros y et z ex hac aequatione $yz-a(y+z)+b=0$ haec forma generalis

$$PP+M(yz-a(y+z)+b)$$

evadet quadratum, cuius ergo species notabiliores evolvamus.

I. Sit $M=2$, ut habeatur

$$PP+2yz-2a(y+z)+2b=\text{quadrato.}$$

Capiatur $P=y-z$ eritque

1) $yy+zz-2a(y+z)+2b=\square$.

Capiatur $P=y-z+a$; erit

2) $yy+zz-4az+2b+aa=\square$,
3) $yy+zz-4ay+2b+aa=\square$.

II. Sit $M=-2$, ut habeatur

$$PP-2yz+2a(y+z)-2b=\text{quadrato.}$$

Capiatur $P = y + z$; erit

4) $yy + zz + 2a(y + z) - 2b = \square$.

Capiatur $P = y + z - a$; erit

5) $yy + zz + aa - 2b = \square$.

III. Sit $M = 2n$, ut habeatur

$$PP + 2nyz - 2na(y + z) + 2nb = \text{quadrato}.$$

Capiatur $P = yz - n$; erit

6) $yyzz - 2na(y + z) + 2nb + nn = \square$.

Capiatur $P = y + z + na$; erit

7) $yy + zz + 2(n + 1)yz + nnaa + 2nb = \square$.

IV. Sit $M = yz + a(y + z) - h$, ut habeatur

$$PP + yyzz - aa(y + z)^2 + (b - h)yz + a(b + h)(y + z) - bh = \text{quadrato}.$$

Capiatur $P = m(y + z) + n$, ut sit

$$yyzz + (mm - aa)(y + z)^2 + (b - h)yz + 2mn(y + z) + nn \\ + a(b + h)(y + z) - bh = \square.$$

Fiat $mn = -\frac{1}{2}a(b + h)$ et $2(mm - aa) + b - h = 0$ sive $n = \frac{a}{m}(aa - mm - b)$ et $h = b + 2(mm - aa)$; erit

8) $yyzz + (mm - aa)(yy + zz) + \frac{aa - mm}{mm}(bb + (aa - 2b)(aa - mm)) = \square$.

COROLLARIUM 1

16. Hinc in aequatione canonica $yz - a(y + z) + b = 0$ litterae a et b ita determinari possunt, ut haec forma

$$yyzz + cc(yy + zz)$$

fiat quadratum. Capiatur enim $mm = aa + cc$ et fiat $bb + 2bcc - aacc = 0$ seu $b = -cc \pm c\sqrt{(aa + cc)}$. Quare pro a eiusmodi sumatur numerus, ut

$aa + cc$ fiat quadratum, tumque erit

$$yz - a(y + z) - cc \pm c\sqrt{(aa + cc)} = 0$$

sive

$$(y - a)(z - a) = aa + cc \pm c\sqrt{(aa + cc)}.$$

At vero hinc conficietur

$$\sqrt{(yyzz + ccyy + cczz)} = (y + z)\sqrt{(aa + cc)} - ac.$$

COROLLARIUM 2

17. Ad formam ergo $yyzz + ccyy + cczz$ quadratum reddendam sumatur primum numerus a, ut $\sqrt{(aa + cc)}$ fiat rationale, eritque tum

$$z = \frac{ay + cc \pm c\sqrt{(aa + cc)}}{y - a}.$$

Haec autem solutio simul praecedentem eiusdem formae in se complectitur casu, quo a capitur infinitum; tum enim oritur $z = -y \pm c$, omnino ut ante, ideoque haec solutio latius patet quam illa.

COROLLARIUM 3

18. Si in forma (8) nulla limitatio fiat, ita ut aequatio proposita $yz - a(y + z) + b = 0$ generatim valeat, ea etiam hoc modo referri potest

$$(yy + mm - aa)(zz + mm - aa) - \frac{mm - aa}{mm}(mm - aa + b)^2 = \text{quadrato}.$$

Quare posito $mm - aa = p$ et $b + p = m = \sqrt{(aa + p)}$ haec aequatio

$$(yy + p)(zz + p) = VV + p$$

resolvetur hac determinatione

$$yz - a(y + z) - p + \sqrt{(aa + p)} = 0,$$

dummodo pro a talis accipiatur numerus, quo $aa + p$ fiat quadratum.

COROLLARIUM 4

19. Si statuatur $\frac{b+p}{m} = q$ seu $b = -p + q\sqrt{(aa+p)}$, ut sit

$$yz - a(y+z) - p + q\sqrt{(aa+p)} = 0,$$

hac determinatione, si modo $aa+p$ fuerit quadratum, satisfiet huic conditioni

$$(yy+p)(zz+p) = VV + pqq;$$

erit autem $V = (y+z)\sqrt{(aa+p)} - aq$.

COROLLARIUM 5

20. Hinc si dato numero p quaerantur numeri y et z, ut fiat

$$(yy+p)(zz+p) = \text{quadrato},$$

posito $q = 0$ huic conditioni satisfiet statuendo $yz - a(y+z) - p = 0$ existente $aa+p$ numero quadrato. Seu sumatur $(y-a)(z-a) = aa+p$, unde, si $aa+p$ in factores resolvatur, commode ambo numeri y et z definiuntur.

COROLLARIUM 6

21. Si sit $a = 0$, forma (8) fiet

$$yyzz + mm(yy+zz) - bb - 2mmb = \square,$$

quae conditio ergo adimplebitur hac aequatione $yz + b = 0$. Facto ergo $b = -2mm$ ista formula

$$yyzz + mmyy + mmzz$$

reddetur quadratum sumendo $yz = 2mm$, quod quidem per se est manifestum.

PROBLEMA 3

22. *Proposita aequatione resolvenda*

$$yy + zz - 2nyz - a = 0$$

invenire formulas notabiliores, quae per eam redduntur quadrata.

SOLUTIO

Hinc ergo ista forma generalis erit quadratum

$$PP + M(yy + zz - 2nyz - a) = \text{quadrato}.$$

I. Sit $M = -1$ et $P = y \pm z$; erit

1) $2(n+1)yz + a = \Box$,

2) $2(n-1)yz + a = \Box$.

II. Sit $M = m$ et $P = yz + mn$; erit

3) $yyzz + myy + mzz - ma + mmnn = \Box$.

III. Sit $M = 2nyz$ et $P = 2nyz$; erit

4) $2nyz(yy + zz) - 2nayz = \Box$.

IV. Sit $M = -zz$ et $P = -zz + nyz + \frac{1}{2}a$[1]; erit

5) $(nn-1)yyzz + nayz + \frac{1}{4}aa = \Box$.

COROLLARIUM 1

23. Si ponamus $a = mnn$, pervenimus ad hanc formam

$$yyzz + myy + mzz,$$

quae ergo redditur quadratum per hanc aequationem

$$yy + zz - 2nyz - mnn = 0,$$

unde fit

$$z = ny \pm \sqrt{((nn-1)yy + mnn)}.$$

Quare pro y talis numerus assumi debet, ut $(nn-1)yy + mnn$ fiat quadratum.

1) Editio princeps (atque etiam *Comment. arithm.*): $P = zz + nyz + \frac{1}{2}a$. Correxit F. R.

COROLLARIUM 2

24. Quoniam hic numerus n arbitrio nostro relinquitur, sumatur talis, ut $nn-1$ prodeat quadratum; sic enim commodissime forma

$$(nn-1)yy+mnn$$

ad quadratum reducetur; capiatur scilicet $n=\frac{kk+1}{2k}$.

SCHOLION

25. Hisce formulis, quae duas indeterminatas involvunt, fusius non immoror, quoniam ex allatis perspicuum est, quomodo huiusmodi formularum investigationem in infinitum extendere liceat. Pergo ergo ad tres indeterminatas, ubi plurima egregia porismata occurrunt, quorum praecipua hic explicabo.

PROBLEMA 4

26. *Proposita hac aequatione resolvenda*

$$a=x+y+z$$

definire formulas notabiliores, quae per eius resolutionem quadrata redduntur.

SOLUTIO

Quadratum ergo generatim erit haec forma

$$PP+M(x+y+z-a).$$

Sit $M=2n$, ut fiat

$$PP+2n(x+y+z)-2na=\Box.$$

Capiatur $P=x-n$; erit

1) $xx+2n(y+z)+nn-2na=\Box$,
2) $yy+2n(x+z)+nn-2na=\Box$,
3) $zz+2n(x+y)+nn-2na=\Box$.

Capiatur $P = x + y - n$; erit

4) $(x + y)^2 + 2nz + nn - 2na = \square$,

5) $(x + z)^2 + 2ny + nn - 2na = \square$,

6) $(y + z)^2 + 2nx + nn - 2na = \square$.

Sit $M = 2nxy$ et $P = xy - nx - ny$; erit

7) $xxyy + 2nxyz + nnxx + nnyy + 2n(n - a)xy = \square$,

8) $xxzz + 2nxyz + nnxx + nnzz + 2n(n - a)xz = \square$,

9) $yyzz + 2nxyz + nnyy + nnzz + 2n(n - a)yz = \square$.

Sit $M = -(a + x + y + z)$ et $P = x + y - z$; erit

10) $aa - 4xz - 4yz = \square$,

11) $aa - 4xy - 4yz = \square$,

12) $aa - 4xy - 4xz = \square$.

Sit $M = -n(a + x + y + z)$ et $P = xy + xz + yz + n$; erit

13) $(xy + xz + yz)^2 - n(xx + yy + zz) + nn + naa = \square$.

COROLLARIUM 1

27. Sit $n = 2a$ et $a = \frac{1}{4}$ atque his conditionibus

$$xx + y + z = \square, \qquad (x + y)^2 + z = \square,$$
$$yy + x + z = \square, \qquad (x + z)^2 + y = \square,$$
$$zz + x + y = \square, \qquad (y + z)^2 + x = \square$$

satisfiet ponendo $x + y + z = \frac{1}{4}$.

COROLLARIUM 2

28. Sit $n = 1 = a$ atque his conditionibus

$$xxyy + 2xyz + xx + yy = \square,$$
$$xxzz + 2xyz + xx + zz = \square,$$
$$yyzz + 2xyz + yy + zz = \square$$

satisfiet ponendo $x + y + z = 1$.

COROLLARIUM 3

29. Sit $a = 2$ atque his conditionibus

$$1 - xz - yz = \square,$$

$$1 - xy - yz = \square,$$

$$1 - xy - xz = \square$$

satisfiet ponendo $x + y + z = 2$.

PROBLEMA 5

30. *Proposita hac aequatione resolvenda*

$$xy + xz + yz = a(x + y + z) + b$$

definire formulas notabiliores, quae per eius resolutionem redduntur quadrata.

SOLUTIO

Erit ergo in genere haec formula

$$PP + M(xy + xz + yz - a(x + y + z) - b) = \text{quadrato}.$$

Sit $M = 2$, ut habeatur

$$PP + 2(xy + xz + yz) - 2a(x + y + z) - 2b = \text{quadrato}.$$

Capiatur $P = x + y + z + a$; erit

1) $xx + yy + zz + 4(xy + xz + yz) + aa - 2b =$ quadrato.

Capiatur $P = x + y - z + a$; erit

2) $xx + yy + zz + 4xy - 4az + aa - 2b = \square$,

3) $xx + yy + zz + 4xz - 4ay + aa - 2b = \square$,

4) $xx + yy + zz + 4yz - 4ax + aa - 2b = \square$.

cuius solutio, si more consueto tentetur, non exiguis difficultatibus implicata deprehenditur; ex quo, si praeterea aliae conditiones praescribantur, quibus simul satisfieri oporteat, quaestio non immerito plus quam determinata ac vires Analyseos transcendens videri debet. Continetur ergo in evolutione huius problematis iam porisma amplissimum, quod in Analysi DIOPHANTEA summum habet usum; quod cum natum sit ex positione simplicissima $z+y=a$, ita formulae magis compositae nos ad profundiora ac magis recondita porismata manuducent.

PROBLEMA 2

15. *Proposita hac aequatione resolvenda*

$$yz-a(y+z)+b=0$$

invenire formulas notabiliores, quae per eius resolutionem redduntur quadrata.

SOLUTIO

Sumta relatione inter numeros y et z ex hac aequatione $yz-a(y+z)+b=0$ haec forma generalis

$$PP+M(yz-a(y+z)+b)$$

evadet quadratum, cuius ergo species notabiliores evolvamus.

I. Sit $M=2$, ut habeatur

$$PP+2yz-2a(y+z)+2b=\text{quadrato.}$$

Capiatur $P=y-z$ eritque

1) $yy+zz-2a(y+z)+2b=\square.$

Capiatur $P=y-z+a$; erit

2) $yy+zz-4az+2b+aa=\square,$

3) $yy+zz-4ay+2b+aa=\square.$

II. Sit $M=-2$, ut habeatur

$$PP-2yz+2a(y+z)-2b=\text{quadrato.}$$

Capiatur $P = y + z$; erit

4) $yy + zz + 2a(y + z) - 2b = \Box$.

Capiatur $P = y + z - a$; erit

5) $yy + zz + aa - 2b = \Box$.

III. Sit $M = 2n$, ut habeatur

$$PP + 2nyz - 2na(y + z) + 2nb = \text{quadrato}.$$

Capiatur $P = yz - n$; erit

6) $yyzz - 2na(y + z) + 2nb + nn = \Box$.

Capiatur $P = y + z + na$; erit

7) $yy + zz + 2(n + 1)yz + nnaa + 2nb = \Box$.

IV. Sit $M = yz + a(y + z) - h$, ut habeatur

$$PP + yyzz - aa(y + z)^2 + (b - h)yz + a(b + h)(y + z) - bh = \text{quadrato}.$$

Capiatur $P = m(y + z) + n$, ut sit

$$yyzz + (mm - aa)(y + z)^2 + (b - h)yz + 2mn(y + z) + nn + a(b + h)(y + z) - bh = \Box.$$

Fiat $mn = -\frac{1}{2}a(b + h)$ et $2(mm - aa) + b - h = 0$ sive $n = \frac{a}{m}(aa - mm - b)$ et $h = b + 2(mm - aa)$; erit

8) $yyzz + (mm - aa)(yy + zz) + \frac{aa - mm}{mm}(bb + (aa - 2b)(aa - mm)) = \Box$.

COROLLARIUM 1

16. Hinc in aequatione canonica $yz - a(y + z) + b = 0$ litterae a et b ita determinari possunt, ut haec forma

$$yyzz + cc(yy + zz)$$

fiat quadratum. Capiatur enim $mm = aa + cc$ et fiat $bb + 2bcc - aacc = 0$ seu $b = -cc \pm c\sqrt{(aa + cc)}$. Quare pro a eiusmodi sumatur numerus, ut

$aa + cc$ fiat quadratum, tumque erit

$$yz - a(y + z) - cc \pm c\sqrt{(aa + cc)} = 0$$

sive

$$(y - a)(z - a) = aa + cc \pm c\sqrt{(aa + cc)}.$$

At vero hinc conficietur

$$\sqrt{(yyzz + ccyy + cczz)} = (y + z)\sqrt{(aa + cc)} - ac.$$

COROLLARIUM 2

17. Ad formam ergo $yyzz + ccyy + cczz$ quadratum reddendam sumatur primum numerus a, ut $\sqrt{(aa + cc)}$ fiat rationale, eritque tum

$$z = \frac{ay + cc \pm c\sqrt{(aa + cc)}}{y - a}.$$

Haec autem solutio simul praecedentem eiusdem formae in se complectitur casu, quo a capitur infinitum; tum enim oritur $z = -y \pm c$, omnino ut ante, ideoque haec solutio latius patet quam illa.

COROLLARIUM 3

18. Si in forma (8) nulla limitatio fiat, ita ut aequatio proposita $yz - a(y + z) + b = 0$ generatim valeat, ea etiam hoc modo referri potest

$$(yy + mm - aa)(zz + mm - aa) - \frac{mm - aa}{mm}(mm - aa + b)^2 = \text{quadrato}.$$

Quare posito $mm - aa = p$ et $b + p = m = \sqrt{(aa + p)}$ haec aequatio

$$(yy + p)(zz + p) = VV + p$$

resolvetur hac determinatione

$$yz - a(y + z) - p + \sqrt{(aa + p)} = 0,$$

dummodo pro a talis accipiatur numerus, quo $aa + p$ fiat quadratum.

COROLLARIUM 4

19. Si statuatur $\frac{b+p}{m}=q$ seu $b=-p+q\sqrt{(aa+p)}$, ut sit

$$yz-a(y+z)-p+q\sqrt{(aa+p)}=0,$$

hac determinatione, si modo $aa+p$ fuerit quadratum, satisfiet huic conditioni

$$(yy+p)(zz+p)=VV+pqq;$$

erit autem $V=(y+z)\sqrt{(aa+p)}-aq$.

COROLLARIUM 5

20. Hinc si dato numero p quaerantur numeri y et z, ut fiat

$$(yy+p)(zz+p)=\text{quadrato},$$

posito $q=0$ huic conditioni satisfiet statuendo $yz-a(y+z)-p=0$ existente $aa+p$ numero quadrato. Seu sumatur $(y-a)(z-a)=aa+p$, unde, si $aa+p$ in factores resolvatur, commode ambo numeri y et z definiuntur.

COROLLARIUM 6

21. Si sit $a=0$, forma (8) fiet

$$yyzz+mm(yy+zz)-bb-2mmb=\square,$$

quae conditio ergo adimplebitur hac aequatione $yz+b=0$. Facto ergo $b=-2mm$ ista formula

$$yyzz+mmyy+mmzz$$

reddetur quadratum sumendo $yz=2mm$, quod quidem per se est manifestum.

PROBLEMA 3

22. *Proposita aequatione resolvenda*

$$yy+zz-2nyz-a=0$$

invenire formulas notabiliores, quae per eam redduntur quadrata.

SOLUTIO

Hinc ergo ista forma generalis erit quadratum

$$PP + M(yy + zz - 2nyz - a) = \text{quadrato}.$$

I. Sit $M = -1$ et $P = y \pm z$; erit

1) $2(n+1)yz + a = \Box$,

2) $2(n-1)yz + a = \Box$.

II. Sit $M = m$ et $P = yz + mn$; erit

3) $yyzz + myy + mzz - ma + mmnn = \Box$.

III. Sit $M = 2nyz$ et $P = 2nyz$; erit

4) $2nyz(yy + zz) - 2nayz = \Box$.

IV. Sit $M = -zz$ et $P = -zz + nyz + \frac{1}{2}a$[1]; erit

5) $(nn-1)yyzz + nayz + \frac{1}{4}aa = \Box$.

COROLLARIUM 1

23. Si ponamus $a = mnn$, pervenimus ad hanc formam

$$yyzz + myy + mzz,$$

quae ergo redditur quadratum per hanc aequationem

$$yy + zz - 2nyz - mnn = 0,$$

unde fit

$$z = ny \pm \sqrt{((nn-1)yy + mnn)}.$$

Quare pro y talis numerus assumi debet, ut $(nn-1)yy + mnn$ fiat quadratum.

1) Editio princeps (atque etiam *Comment. arithm.*): $P = zz + nyz + \frac{1}{2}a$. Correxit F. R.

COROLLARIUM 2

24. Quoniam hic numerus n arbitrio nostro relinquitur, sumatur talis, ut $nn-1$ prodeat quadratum; sic enim commodissime forma

$$(nn-1)yy+mnn$$

ad quadratum reducetur; capiatur scilicet $n=\frac{kk+1}{2k}$.

SCHOLION

25. Hisce formulis, quae duas indeterminatas involvunt, fusius non immoror, quoniam ex allatis perspicuum est, quomodo huiusmodi formularum investigationem in infinitum extendere liceat. Pergo ergo ad tres indeterminatas, ubi plurima egregia porismata occurrunt, quorum praecipua hic explicabo.

PROBLEMA 4

26. *Proposita hac aequatione resolvenda*

$$a=x+y+z$$

definire formulas notabiliores, quae per eius resolutionem quadrata redduntur.

SOLUTIO

Quadratum ergo generatim erit haec forma

$$PP+M(x+y+z-a).$$

Sit $M=2n$, ut fiat

$$PP+2n(x+y+z)-2na=\square.$$

Capiatur $P=x-n$; erit

1) $xx+2n(y+z)+nn-2na=\square$,
2) $yy+2n(x+z)+nn-2na=\square$,
3) $zz+2n(x+y)+nn-2na=\square$.

Capiatur $P = x + y - n$; erit

4) $(x+y)^2 + 2nz + nn - 2na = \square$,

5) $(x+z)^2 + 2ny + nn - 2na = \square$,

6) $(y+z)^2 + 2nx + nn - 2na = \square$.

Sit $M = 2nxy$ et $P = xy - nx - ny$; erit

7) $xxyy + 2nxyz + nnxx + nnyy + 2n(n-a)xy = \square$,

8) $xxzz + 2nxyz + nnxx + nnzz + 2n(n-a)xz = \square$,

9) $yyzz + 2nxyz + nnyy + nnzz + 2n(n-a)yz = \square$.

Sit $M = -(a + x + y + z)$ et $P = x + y - z$; erit

10) $aa - 4xz - 4yz = \square$,

11) $aa - 4xy - 4yz = \square$,

12) $aa - 4xy - 4xz = \square$.

Sit $M = -n(a + x + y + z)$ et $P = xy + xz + yz + n$; erit

13) $(xy + xz + yz)^2 - n(xx + yy + zz) + nn + naa = \square$.

COROLLARIUM 1

27. Sit $n = 2a$ et $a = \frac{1}{4}$ atque his conditionibus

$$xx + y + z = \square, \qquad (x+y)^2 + z = \square,$$
$$yy + x + z = \square, \qquad (x+z)^2 + y = \square,$$
$$zz + x + y = \square, \qquad (y+z)^2 + x = \square$$

satisfiet ponendo $x + y + z = \frac{1}{4}$.

COROLLARIUM 2

28. Sit $n = 1 = a$ atque his conditionibus

$$xxyy + 2xyz + xx + yy = \square,$$
$$xxzz + 2xyz + xx + zz = \square,$$
$$yyzz + 2xyz + yy + zz = \square$$

satisfiet ponendo $x + y + z = 1$.

COROLLARIUM 3

29. Sit $a = 2$ atque his conditionibus

$$1 - xz - yz = \square,$$

$$1 - xy - yz = \square,$$

$$1 - xy - xz = \square$$

satisfiet ponendo $x + y + z = 2$.

PROBLEMA 5

30. *Proposita hac aequatione resolvenda*

$$xy + xz + yz = a(x + y + z) + b$$

definire formulas notabiliores, quae per eius resolutionem redduntur quadrata.

SOLUTIO

Erit ergo in genere haec formula

$$PP + M(xy + xz + yz - a(x + y + z) - b) = \text{quadrato.}$$

Sit $M = 2$, ut habeatur

$$PP + 2(xy + xz + yz) - 2a(x + y + z) - 2b = \text{quadrato.}$$

Capiatur $P = x + y + z + a$; erit

1) $xx + yy + zz + 4(xy + xz + yz) + aa - 2b = \text{quadrato.}$

Capiatur $P = x + y - z + a$; erit

2) $xx + yy + zz + 4xy - 4az + aa - 2b = \square,$

3) $xx + yy + zz + 4xz - 4ay + aa - 2b = \square,$

4) $xx + yy + zz + 4yz - 4ax + aa - 2b = \square.$

Capiatur $P = x - y$; erit

5) $xx + yy + 2(x + y)z - 2a(x + y + z) - 2b = \square$,

6) $xx + zz + 2(x + z)y - 2a(x + y + z) - 2b = \square$,

7) $yy + zz + 2(y + z)x - 2a(x + y + z) - 2b = \square$.

Sit $M = -2$ et $P = x + y + z - a$; erit

8) $xx + yy + zz + aa + 2b = \square$.

PROBLEMA 6

31. *Proposita hac aequatione*

$$xx + yy + zz = 2xy + 2xz + 2yz + a$$

definire formulas simpliciores, quae per eius resolutionem quadrata redduntur.

SOLUTIO

In genere ergo haec formula erit

$$PP + M(xx + yy + zz - 2xy - 2xz - 2yz - a) = \text{quadrato.}$$

Sit $M = -1$ ac ponatur $P = x + y + z$; erit

1) $4xy + 4xz + 4yz + a = \square$.

Sit $M = -1$ et $P = x + y - z$; erit

2) $4xy + a = \square$,

3) $4xz + a = \square$,

4) $4yz + a = \square$.

Sit $M = -1$ et $P = x - y$; erit

5) $a + 2(x + y)z - zz = \square$,

6) $a + 2(x + z)y - yy = \square$,

7) $a + 2(y + z)x - xx = \square$.

COROLLARIUM 1

32. Posito $a = 4n$, ut sit

$$xx + yy + zz = 2xy + 2xz + 2yz + 4n,$$

fient simul sequentes formulae quadrata:

$$xy + n = \square,$$

$$xz + n = \square,$$

$$yz + n = \square$$

et

$$xy + xz + yz + n = \square.$$

Unde haec elegans quaestio DIOPHANTEA[1]) resolvitur:

Dato numero quocunque n invenire tres numeros, ut producta ex binis singula illo numero aucta fiant quadrata; quibus conditionibus adiungi potest haec, ut summa productorum ex binis eodem numero aucta quoque fiat quadratum.

COROLLARIUM 2

33. Cum enim ex aequatione sit

$$z = x + y \pm 2\sqrt{(xy + n)},$$

sumantur pro x et y tales numeri, quibus $xy + n$ reddatur quadratum, puta $xy + n = uu$; indeque elicietur duplex valor pro numero z, scilicet

$$z = x + y \pm 2u,$$

quorum uterque cum x et y omnibus conditionibus aeque satisfacit.

COROLLARIUM 3

34. Cum autem sit $\sqrt{(xy + n)} = u$, erunt sumto tertio numero $z = x + y + 2u$ reliquae formulae

1) Cf. quaestionem X libri III DIOPHANTI *Arithmeticorum* (ed. TANNERY; quae quaestio est quaestio XII editionis BACHETI); vide notam p. 404 huius voluminis. Vide etiam L. EULER, *Vollständige Anleitung zur Algebra*, l. c. § 231 et 232. F. R.

$$\sqrt{(xz+n)} = \frac{x+z-y}{2} = x+u,$$

$$\sqrt{(yz+n)} = \frac{y+z-x}{2} = y+u,$$

$$\sqrt{(xy+xz+yz+n)} = \frac{x+y+z}{2} = x+y+u.$$

PROBLEMA 7

35. *Proposita hac aequatione*

$$xx+yy+zz = 2xy+2xz+2yz+2a(x+y+z)+b$$

definire formulas notabiliores, quae per eius resolutionem redduntur quadrata.

SOLUTIO

In genere ergo quadratum erit haec forma

$$PP+M(xx+yy+zz-2xy-2xz-2yz-2a(x+y+z)-b).$$

Sit $M=-1$ et capiatur $P=x+y+z+a$; erit

1) $4xy+4xz+4yz+4a(x+y+z)+aa+b=\square$.

Capiatur $P=x+y+z-a$; erit

2) $4xy+4xz+4yz+aa+b=\square$.

Capiatur $P=x+y-z+a$; erit

3) $4xy+4a(x+y)+aa+b=\square$,

4) $4xz+4a(x+z)+aa+b=\square$,

5) $4yz+4a(y+z)+aa+b=\square$.

Capiatur $P=x+y-z-a$; erit

6) $4xy+4az+aa+b=\square$,

7) $4xz+4ay+aa+b=\square$,

8) $4yz+4ax+aa+b=\square$.

COROLLARIUM 1

36. Ad formulas has facillime solvendas ponatur tertia

$$4xy+4a(x+y)+aa+b$$

aequalis quadrato cuipiam uu et ob $4(x+a)(y+a)=uu-b+3aa$ seu

$$(x+a)(y+a)=\frac{1}{4}(uu-b+3aa)$$

ex factoribus numeri $\frac{1}{4}(uu-b+3aa)$ commodissime definiuntur numeri duo x et y; tertius autem z colligitur ex formae tertiae radice quadrata $x+y-z+a$, quae ergo est $=u$, unde fit $z=x+y+a\pm u$.

COROLLARIUM 2

37. Si sit $b=-aa$, per resolutionem huius aequationis

$$xx+yy+zz=2xy+2xz+2yz+2a(x+y+z)-aa$$

sequentes formulae omnes in quadrata abibunt:

$$xy+a(x+y)=\square, \quad xy+az=\square,$$

$$xz+a(x+z)=\square, \quad xz+ay=\square,$$

$$yz+a(y+z)=\square, \quad yz+ax=\square,$$

$$xy+xz+yz=\square,$$

$$xy+xz+yz+a(x+y+z)=\square.$$

Satisfiet autem sumendo

$$z=x+y+a\pm 2\sqrt{(xy+a(x+y))}=x+y+a\pm 2u$$

posito $(x+a)(y+a)=uu+aa$.

COROLLARIUM 3

38. In hoc corollario continetur illud ipsum problema, cuius initio feci mentionem, siquidem ponatur $a=1$. Atque ex iisdem formulis solvi quoque potest quaestio, in qua ipsi numeri x, y, z quadrati esse debent, cuius solutionem hic subiungam.

QUAESTIO

39. *Invenire tres numeros quadratos, ut, ad productum binorum sive eorundem summa sive reliquus addatur, quadratum prodeat atque ut insuper tam summa productorum ex binis ipsa quam eadem, summa numerorum aucta, fiat quadratum.*[1])

Positis ergo xx, yy, zz quadratis, qui quaeruntur, sequentes formulas quadrata reddi oportet:

$$xxyy + xx + yy = \square, \qquad xxyy + zz = \square,$$
$$xxzz + xx + zz = \square, \qquad xxzz + yy = \square,$$
$$yyzz + yy + zz = \square, \qquad yyzz + xx = \square,$$
$$xxyy + xxzz + yyzz = \square,$$
$$xxyy + xxzz + yyzz + xx + yy + zz = \square.$$

His autem omnibus satisfit, dummodo statuatur

$$zz = xx + yy + 1 \pm 2\sqrt{(xxyy + xx + yy)}.$$

Supra [§ 12] autem vidimus formam $xxyy + xx + yy$ quadratum fieri, si ponatur $y = x + 1$. Sit igitur $y = x + 1$ eritque

$$zz = 2xx + 2x + 2 \pm 2\sqrt{(x^4 + 2x^3 + 3xx + 2x + 1)}$$

seu

$$zz = 4(xx + x + 1).$$

Tantum ergo superest, ut $xx + x + 1$ reddatur quadratum, quod posita radice $-x + t$ praebet

$$x = \frac{tt - 1}{2t + 1}$$

et

$$\sqrt{(xx + x + 1)} = \frac{tt + t + 1}{2t + 1},$$

unde fit

$$z = 2\sqrt{(xx + x + 1)} = \frac{2(tt + t + 1)}{2t + 1}.$$

Quadratorum ergo trium quaesitorum radices sunt

$$x = \frac{tt - 1}{2t + 1}, \quad y = \frac{tt + 2t}{2t + 1}, \quad z = \frac{2tt + 2t + 2}{2t + 1}.$$

---

1) Cf. quaestionem V libri V DIOPHANTI *Arithmeticorum* (ed. TANNERY); vide notam p. 404 huius voluminis. F. R.

Vel quo facilius pro t fractiones capi queant, statuatur

$$t = \frac{r-q}{2q}$$

eruntque hae radices

$$x = \frac{3qq+2qr-rr}{4qr}\text{[1]}, \quad y = \frac{rr+2qr-3qq}{4qr}, \quad z = \frac{rr+3qq}{2qr},$$

unde sumto $r = 2$ et $q = 1$ oriuntur hi valores

$$x = \frac{3}{8}, \quad y = \frac{5}{8}, \quad z = \frac{7}{4},$$

quibus solutio [prima] supra[2]) tradita continetur. Simplicior fortasse solutio [quarta] est

$$x = \frac{3}{5}, \quad y = \frac{8}{5} \quad \text{et} \quad z = \frac{14}{5}.$$

SCHOLION

40. His praeceptis observandis facile erit numerum talium formularum pro lubitu multiplicare easque tam ad quatuor indeterminatas quam ad formas magis compositas extendere. Quin etiam simili modo plures formae exhiberi poterunt, quae per certam positionem cubi redduntur; sed quoniam in iis non amplius tanta cernitur concinnitas, hanc meditationem finiendam esse censeo, cum id, quod mihi praecipue erat propositum, ut novum Analyseos DIOPHANTEAE supplementum producerem, abunde explicaverim.

1) Recte quidem ex substitutione $t = \frac{r-q}{2q}$ computatur $x = \frac{rr-2qr-3qq}{4qr}$, qui valor etiam cum aequatione $y = x+1$ consentit. Quia autem hac in quaestione de quadratis solum numerorum x, y, z agitur, signa numerorum ipsorum nullius momenti sunt. F. R.

2) Vide solutiones p. 404 in numeris quadratis expositas. Solutio quarta obtinetur sumto $r = 5$ et $q = 1$. F. R.

SOLUTIO GENERALIS QUORUNDAM PROBLEMATUM DIOPHANTEORUM QUAE VULGO NONNISI SOLUTIONES SPECIALES ADMITTERE VIDENTUR[1]

Commentatio 255 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 6 (1756/7), 1761, p. 155—184
Summarium ibidem p. 17—18

SUMMARIUM

Quanta utilitas a methodo DIOPHANTEA dicta, si uberius excolatur, in universam Analysin sit redundatura, a Cel. Auctore huius dissertationis iam saepius est commemoratum, unde ipsum in hac Analyseos parte diu multumque desudasse minime poenitet. Hic autem imprimis observat omnia huius generis problemata, prouti adhuc sunt tractata, quasi sponte in duas classes distribui. Vel enim problemata ita sunt comparata, ut omnes omnino solutiones in iisdem formulis generalibus contineantur sicque tota solutio una quasi operatione absolvatur, cuiusmodi problemata in unam classem coniicienda videntur; vel problemata eius sunt naturae, ut omnes solutiones non in una expressione generali comprehendi queant, sed tantum ex solutionibus iam inventis continuo novas alias elicere liceat, etiamsi forte eiusmodi formulae exhiberi queant, quae infinitas quidem solutiones, attamen non omnes in se complectantur; talia problemata alteram classem constituent.

Ad classem priorem pertinet exempli causa problema, quo duo quadrata quaeruntur, quorum summa itidem sit quadratum, ubi constat omnium huiusmodi quadratorum radices formulis generalibus exprimi posse. Ad classem vero posteriorem ex omnium Auctorum

1) Cf. quoque L. EULER, *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, Zweyter Theil, zweyter Abschnitt, Cap. 15; *LEONHARDI EULERI Opera omnia*, series I, vol. 1. F. R.

sententia referendum est problema de tribus cubis inveniendis, quorum summa sit quoque cubus, ubi quidem formulae pro radicibus horum cuborum dari possunt innumerabiles solutiones suppeditantes, verumtamen semper iis aliae innumerabiles solutiones excluduntur aeque satisfacientes; at ex inventis iam tribus quibusque huiusmodi cubis innumerabiles aliae novae solutiones derivari possunt.

Discrimen inter has duas classes etiam ita essentiale est visum, ut nullius quaestionis ad posteriorem pertinentis solutio generalis exhiberi posse putaretur. Hanc igitur opinionem Auctor in ista dissertatione evertit, dum ostendit idem problema de tribus cubis, quorum summa sit cubus, ita per formulas generales resolvi posse, in quibus omnes omnino solutiones contineantur; methodus autem, qua ad has formulas pervenit, prorsus est singularis ac plurima alia insignia incrementa huius Analyseos partis polliceri videtur.

1. Analysis Diophantea, quae in problematibus indeterminatis per numeros rationales vel etiam integros solvendis versatur, duplicis generis problemata tractare solet, quorum discrimen in ratione solutionis maxime est positum. Alia enim problemata ita sunt comparata, ut solutiones generales exhiberi queant, quae omnes plane numeros satisfacientes in se complectuntur; alia vero nonnisi solutiones particulares admittunt, vel saltem per methodos cognitas nonnisi tales solutiones eruere licet, ita ut praeter numeros, qui forte reperiuntur, infiniti alii problemati satisfacientes existant, qui in solutione inventa non contineantur. Ubi quidem in genere notari convenit prioris ordinis problemata multo facilius resolvi quam ea, quae ad alterum ordinem referuntur, quippe quae plerumque singularem sagacitatem cum eximiis artificiis coniunctam requirunt, in quibus maxima vis huius Analysis cernitur. Quare ob hanc causam problemata Diophantea in has duas classes distribui debere videntur.

2. Diophantus quidem ipse omnium quaestionum, quas tractat, solutiones tantum specialissimas tradit numerosque, quibus unica solutio continetur, plerumque indicasse est contentus. Neque vero eius methodus ad has solutiones specialissimas adstricta est putanda; quia enim tunc temporis usus litterarum, quibus numeri indefiniti designentur, nondum erat receptus, huiusmodi solutiones latius patentes, quales nunc quidem exhiberi solent, ab ipso expectari non poterant; interim tamen ipsae methodi, quibus ad quaelibet problemata solvenda utitur, aeque late patent quam eae, quae hodie sunt in

usu; quin etiam fateri cogimur vix ullam in hoc Analyseos genere adhuc esse inventam, cuius vestigia satis luculenta non iam in ipso DIOPHANTO deprehendantur. Non obstante igitur hac apparente particularitate solutionum DIOPHANTEARUM disparitas problematum supra memorata in ipso iam DIOPHANTO manifesto cernitur, siquidem ad methodos eius respiciamus; quarum aliae ita sunt comparatae, ut omnes omnino solutiones, quae problemati satisfacere possunt, suppeditare queant, aliae vero nonnullas tantum solutiones praebeant vel, etiamsi earum numerus in infinitum augeri possit, tamen in iis innumerabiles aliae, quae aeque satisfaciunt, non contineantur.

3. Exemplum problematis, cuius solutio generalis exhiberi potest, praebet quaestio vulgata, qua quaeruntur duo numeri quadrati, quorum summa sit quadratum, sive sumtis x et y pro radicibus istorum quadratorum ut $xx+yy$ sit numerus quadratus. Sumtis enim pro lubitu tribus numeris a, p et q haec habebitur solutio generalis

$$y=2apq \quad \text{et} \quad x=a(pp-qq);$$

ex his namque valoribus prodit

$$\sqrt{(xx+yy)}=a(pp+qq).$$

De qua solutione tenendum est nullos plane dari numeros pro x et y substituendos, quorum quadratorum summa fiat quadratum, qui non simul in formulis datis contineantur. Atque haec generalitas non solum inde perspicitur, quod pro tribus litteris a, p et q numeros quoscunque accipere liceat, unde iam infinities infinita solutionum multitudo obtinetur, sed etiam ipsa harum formularum investigatio evincit nullam plane dari solutionem, quae non in iis comprehendatur. At vero hoc posterius criterium longe certius est priori, cum saepe multae litterae indefinitae in solutionem ingredi queant neque tamen solutio propterea reddatur generalis.

4. Investigationis autem ratio in hoc exemplo nobis solutionis universalitatem plane ostendit. Cum enim $\sqrt{(xx+yy)}$ debeat esse numerus rationalis, is certe erit maior quam x; statuatur ergo $=x+z$. Tum vero, quaecunque sit ratio ipsius y ad z, poni poterit $z=\frac{q}{p}y$ neque hoc modo generalitas positionis limitatur. Posito autem $\sqrt{(xx+yy)}=x+\frac{q}{p}y$ sumtis qua-

dratis habebimus

$$xx + yy = xx + \frac{2q}{p}xy + \frac{qq}{pp}yy.$$

Deleto utrinque termino xx ac residuo per y diviso prodibit

$$y = \frac{2q}{p}x + \frac{qq}{pp}y \quad \text{seu} \quad (pp - qq)y = 2pqx.$$

Erit ergo

$$\frac{x}{y} = \frac{pp - qq}{2pq}$$

hincque x et y sunt vel aeque multipla vel aeque submultipla numerorum $pp - qq$ et $2pq$. Sumta ergo a pro indice generali sive multiplorum sive submultiplorum nanciscemur

$$y = 2apq \quad \text{et} \quad x = a(pp - qq)$$

et ob $z = \frac{q}{p}y = 2aqq$ erit

$$x + z = \sqrt{(xx + yy)} = a(pp + qq).$$

5. Problematis autem, cuius solutio per methodos cognitas generalis exhiberi nequit, exemplum esto quaestio de inveniendis tribus cubis, quorum summa sit cubus; sive quaerendi sint tres numeri x, y et z, ita ut sit

$$x^3 + y^3 + z^3 = \text{cubo}.$$

Quod problema cum ab ipso DIOPHANTO[1]) tum a recentioribus[2]) pluribus modis

1) Cf. quaestionem II libri IV, imprimis autem porisma commemoratum in quaestione XVI (= XIX editionis BACHETI) libri V DIOPHANTI *Arithmeticorum* (ed. TANNERY); vide notam p. 404 huius voluminis. F. R.

2) Vide FR. VIETA, *Zeteticorum* liber IV, Zetetica 18—20, *Opera mathematica* (ed. FR. v. SCHOOTEN), Lugd. Batav. 1646, p. 74—75. Vide porro BACHETI commentarios in DIOPHANTI *Arithmeticorum* quaestiones nota praecedente laudatas, imprimis autem FERMATII observationes ad hos commentarios (cf. notam 2 p. 51 huius voluminis), *Oeuvres de FERMAT*, t. I, p. 297—299 et 315—318. Vide etiam J. DE BILLY (1602—1679), *Doctrinae analyticae inventum novum, collectum ex variis D. DE FERMAT epistolis*, quam collectionem FERMATIUS minor in DIOPHANTI *Arithmeticorum* editione tolosana a. 1670 publicavit (cf. notam 2 p. 51 huius voluminis), *Oeuvres de FERMAT*, t. III, p. 325, imprimis p. 345—346, nec non *JACOBI DE BILLY Doctrinae analyticae*

extat solutum atque ita quidem, ut infinita multitudo solutionum sit exhibita; neque tamen ulla solutio tam late patet, ut omnes plane casus huic quaestioni satisfacientes in se complectatur. In hoc problemate etiam vel unus cubus x^3 vel duo x^3+y^3 tanquam dati spectari possunt, unde vel duos reliquos cubos vel unicum quaeri oportet, ut summa fiat cubus; quomodocunque autem solutio instituatur, tamen maxime particularis evadit.

6. Quod quo clarius perspiciatur, solutiones dari solitas hic breviter commemoremus. Sint igitur primo dati duo cubi a^3 et b^3 tertiumque x^3 inveniri oporteat, ut omnium trium summa

$$a^3+b^3+x^3$$

denuo fiat cubus. Manifestum iam quidem est radicem huius cubi maiorem fore quam x; sed etiamsi statuatur $=x+v$, tamen aequatio quadratica pro inveniendo x prodit sicque difficultas non diminuitur. Poni igitur solet $x=p-b$, ut summa trium cuborum fiat

$$a^3+3bbp-3bpp+p^3=\text{cubo}=v^3,$$

atque hac quidem positione amplitudo solutionis non restringitur. Porro autem eiusmodi cubus assumi debet, ut incognita p per aequationem simplicem ideoque rationaliter exhiberi queat. Manifestum autem est hoc duplici modo fieri posse. Primo enim sumto $v=a+p$ fiet

$$a^3+3bbp-3bpp+p^3=a^3+3aap+3app+p^3;$$

ubi cum termini a^3 et p^3 se destruant, reliquum per $3p$ divisum dat

$$bb-bp=aa+ap \quad \text{ideoque} \quad p=\frac{bb-aa}{a+b}=b-a,$$

---

inventum novum. FERMATS Briefen an BILLY entnommen. Herausgegeben und übersetzt von P. v. SCHAEWEN, Berlin 1910, p. 19—20, 74—75, 126. Cf. quoque epistolas, quas a. 1657/8 BROUNCKER ad WALLIS atque WALLIS et FRENICLE ad KENELMUM DIGBY scripserunt (epist. X, XVI, XXVI, XXVIII *Commercii epistolici* a WALLISIO a. 1658 primo editi), I. WALLIS *Opera*, t. II, Oxoniae 1693, p. 768, 777, 820, 824; *Oeuvres de FERMAT*, t. III, p. 419, 427, 530, 537, imprimis p. 420, 436, 535, 538. — Vide praeterea T. L. HEATH, *DIOPHANTUS of Alexandria. A study in the history of greek algebra.* Second edition. With a supplement containing an account of FERMAT's theorems and problems connected with DIOPHANTINE analysis and some solutions of DIOPHANTINE problems by EULER, Cambridge 1910, p. 168, 213, 214, 329—334. F. R.

unde fit $x = p - b = -a$, quo casu utique fit

$$a^3 + b^3 + x^3 = a^3 + b^3 - a^3 = b^3 = \text{cubo}.$$

7. Hanc autem solutionem maxime particularem esse ex assumtione valoris $v = a + p$ evidens est, cum ubique fieri possit, ut quantitas

$$a^3 + 3bbp - 3bpp + p^3$$

sit cubus, cuius radix non sit $a + p$, ita ut hac restrictione solutio maxime sit limitata, unde factum est, ut etiam unicum valorem pro p ac proinde pro x exhibuerit, qui adeo ne solutionem quidem idoneam suppeditasse est censendus, propterea quod invenimus $x = -a$, qui casus tam est obvius sua sponte, ut ne pro solutione quidem admitti queat. Pro v igitur alius valor fingi solet, talis tamen, ut inventio ipsius p ad aequationem simplicem perducat, quod usu venit ponendo $v = a + \frac{bb}{aa}p$; fiet enim

$$a^3 + 3bbp - 3bpp + p^3 = a^3 + 3bbp + \frac{3b^4}{a^3}pp + \frac{b^6}{a^6}p^3,$$

quae utrinque deletis terminis $a^3 + 3bbp$ per pp divisa dat

$$-3b + p = \frac{3b^4}{a^3} + \frac{b^6}{a^6}p \qquad \text{seu} \qquad p = \frac{3a^6b + 3a^3b^4}{a^6 - b^6}.$$

8. Cum igitur hinc invenerimus

$$p = \frac{3a^3b(a^3 + b^3)}{a^6 - b^6} = \frac{3a^3b}{a^3 - b^3},$$

erit

$$x = p - b = \frac{2a^3b + b^4}{a^3 - b^3} = \frac{b(2a^3 + b^3)}{a^3 - b^3},$$

quae est radix tertii cubi ad duos datos $a^3 + b^3$ addendi, ut summa fiat cubus. Erit autem summae radix cubica per hypothesin

$$= v = a + \frac{bb}{aa}p = a + \frac{3ab^3}{a^3 - b^3}$$

sive

$$v = \frac{a^4 + 2ab^3}{a^3 - b^3} = \frac{a(a^3 + 2b^3)}{a^3 - b^3}.$$

Quicunque ergo numeri pro a et b fuerint assumti, hinc habebuntur tres cubi, quorum summa est cubus. Hi scilicet erunt[1])

$$a^3 + b^3 + \left(\frac{b(2a^3+b^3)}{a^3-b^3}\right)^3 = \left(\frac{a(a^3+2b^3)}{a^3-b^3}\right)^3.$$

Verum et hanc solutionem maxime esse specialem ex ipsa investigatione perspicuum est, cum plane pro arbitrio nostro radicem trium cuborum [summae] finxerimus $v = a + \frac{bb}{aa}p$, cum sine dubio infinitos quoque alios valores recipere possit.

9. Porro autem datis duobus cubis unicus reperitur tertius cubus, qui cum iis coniunctus producat cubum; manifestum autem est infinitos huiusmodi dari cubos. Si enim sit $a = 4$ et $b = 3$, radix tertii cubi hinc prodit

$$x = \frac{3(2\cdot 64+27)}{64-27} = \frac{465}{37} \quad \text{et} \quad v = \frac{472}{37},$$

ita ut sit

$$4^3 + 3^3 + \left(\frac{465}{37}\right)^3 = \left(\frac{472}{37}\right)^3.$$

Novimus autem cubum quinarii ad hos cubos $4^3 + 3^3$ additum quoque producere cubum, scilicet senarii[2]), seu esse

$$3^3 + 4^3 + 5^3 = 6^3,$$

qui tamen casus in hac solutione non continetur. Quare si ad hoc problema solvendum, ut sit $x^3 + y^3 + z^3 = v^3$, quis dicat sumi debere

$$x = a, \quad y = b \quad \text{et} \quad z = \frac{b(2a^3+b^3)}{a^3-b^3}$$

tumque fore $v = \frac{a(a^3+2b^3)}{a^3-b^3}$, hae formulae quidem satisfaciunt, sed etiamsi ob duos numeros a et b arbitrio nostro relictos infinities infiniti cuborum terniones hinc exhiberi possunt, quorum summa faciat cubum, tamen infiniti alii existunt cuborum terniones idem praestantes, qui in istis formulis non sunt contenti, veluti hic casus $x = 3$, $y = 4$ et $z = 5$, pro quo fit $v = 6$.

1) Formula sequens iam a Fr. Vieta exposita est; vide (l. c.) Zeteticum 18. F. R.

2) Etiam haec formula invenitur apud Fr. Vieta; vide (l. c.) Zeteticum 18. Zetetica sequentia continent praeterea formulas $7^3 + 14^3 + 17^3 = 20^3$ et $252^3 + 248^3 = 5^3 + 315^3$, quarum prior infra (§ 26) etiam ab Eulero exposita est. Ex formula autem posteriore apparet haec Jacobi de Billy (ed. P. v. Schaewen, p. 19; vide notam 2 p. 431 huius voluminis) verba: „Non satis caute negavit Vieta numerum compositum ex duobus cubis posse dividi in alios duos cubos" cum veritate non congruere. F. R.

10. Latius quidem patens reperitur solutio, si unicus tantum trium cuborum quasi datus assumatur, ita ut fieri oporteat

$$a^3 + x^3 + y^3 = v^3.$$

Ponatur hunc in finem $x = pu + r$ et $y = qu - r$, qua quidem positione nulla restrictio inducitur, fietque

$$a^3 + 3rr(p+q)u + 3r(pp-qq)uu + (p^3+q^3)u^3 = v^3.$$

Iam ut quantitas u hinc rationaliter definiri queat, fingatur $v = a + \frac{rr}{aa}(p+q)u$, qua positione utique solutio iam vehementer limitatur; ex ea autem obtinebitur

$$v^3 = a^3 + 3rr(p+q)u + \frac{3r^4}{a^3}(p+q)^2uu + \frac{r^6}{a^6}(p+q)^3u^3.$$

Deletis ergo utrinque terminis $a^3 + 3rr(p+q)u$ et residuo per $(p+q)uu$ diviso emerget haec aequatio

$$3r(p-q) + (pp-pq+qq)u = \frac{3r^4}{a^3}(p+q) + \frac{r^6}{a^6}(p+q)^2u,$$

ex qua eruitur

$$u = \frac{3a^3r^4(p+q) - 3a^6r(p-q)}{a^6(pp-pq+qq) - r^6(p+q)^2}.$$

11. Valore ergo hoc pro u invento erit

$$x = pu + r = \frac{3a^3pr^4(p+q) - a^6r(2pp-2pq-qq) - r^7(p+q)^2}{a^6(pp-pq+qq) - r^6(p+q)^2},$$

$$y = qu - r = \frac{3a^3qr^4(p+q) - a^6r(pp+2pq-2qq) + r^7(p+q)^2}{a^6(pp-pq+qq) - r^6(p+q)^2}$$

et

$$v = a + \frac{rr}{aa}(p+q)u = \frac{a^7(pp-pq+qq) - 3a^4r^3(pp-qq) + 2ar^6(p+q)^2}{a^6(pp-pq+qq) - r^6(p+q)^2}.$$

Cum igitur quatuor litterae a, p, q et r pro arbitrio assumi queant, haec solutio utique infinities latius patet quam praecedens, ubi duae tantum litterae arbitrio nostro relinquebantur. Verumtamen notandum est rationem tantum litterarum p et q in computum ingredi, ita ut hinc litterae arbitrariae ad tres tantum reducantur; nihilo vero minus et haec solutio ob limitationem

circa radicem v adhibitam pro particulari est habenda, ita ut terniones cuborum existant in his formulis non contenti. Solutio autem antecedens ex hac emergit sumto $p=0$, ita ut haec infinities illa sit generalior.

12. Adhuc generaliorem autem obtinebimus, si nullum trium cuborum tanquam cognitum assumamus seu in genere quaeramus x, y et z, ut sit

$$x^3+y^3+z^3=v^3.$$

In hunc finem ponatur

$$x=pt+u,\quad y=-pt+qu \quad \text{et} \quad z=t-qu,$$

quibus positionibus nihil adhuc limitatur; facta autem substitutione oritur

$$\begin{aligned} t^3 &+ 3ppttu + 3ptuu + u^3 = v^3. \\ &+ 3ppqttu - 3pqqtuu \\ &- 3qttu + 3qqtuu. \end{aligned}$$

Iam fingatur $v=t+u$, unde quidem maxima limitatio nascitur, et aequatione per $3tu$ divisa reperietur

$$(pp+ppq-q)t+(p-pqq+qq)u=t+u$$

seu

$$\frac{t}{u}=\frac{-1+p+qq-pqq}{1+q-pp-ppq},$$

capi ergo poterit

$$t=n(-pqq+qq+p-1) \quad \text{et} \quad u=n(-ppq-pp+q+1),$$

unde elicitur

$$\begin{aligned} x&=n(-ppqq+pqq-ppq-p+q+1),\\ y&=n(p+q-pp+qq-ppq-pqq),\\ z&=n(+ppqq-pqq+ppq+p-q-1),\\ v&=n(-pqq-ppq-pp+qq+p+q). \end{aligned}$$

Hinc autem fit $z=-x$ et $v=y$, qui est casus per se obvius.

13. Sequenti autem modo solutio latius patens eruitur. Ponatur

$$x = mt + pu, \quad y = nt + qu \quad \text{et} \quad z = -nt + ru$$

eritque

$$\begin{aligned} x^3 + y^3 + z^3 = m^3t^3 &+ 3mmpttu + 3mpptuu + p^3u^3; \\ &+ 3nnq \quad\; + 3nqq \quad\; + q^3 \\ &+ 3nnr \quad\; - 3nrr \quad\; + r^3 \end{aligned}$$

quae summa cum debeat esse cubus $= v^3$, ponatur

$$v = mt + \frac{mmp + nn(q + r)}{mm}u$$

eritque dividendo per uu

$$3t(mpp + n(qq - rr)) + u(p^3 + q^3 + r^3)$$
$$= \frac{3t}{m^3}(mmp + nn(q + r))^2 + \frac{u}{m^6}(mmp + nn(q + r))^3$$

sicque neglecto communi factore, qui ab arbitrio nostro pendet, erit

$$t = m^6(p^3 + q^3 + r^3) - (mmp + nn(q + r))^3,$$
$$u = 3m^3(mmp + nn(q + r))^2 - 3m^6(mpp + n(qq - rr));$$

quae formae si denuo per communem factorem $q + r$ dividantur, prodit

$$t = m^6(qq - qr + rr) - 3m^4nnpp - 3mmn^4p(q + r) - n^6(q + r)^2,$$
$$u = -3m^6n(q - r) + 6m^5nnp + 3m^3n^4(q + r).$$

14. Hinc iam pro x, y, z emergunt sequentes erpressiones:

$$x = m^7(qq - qr + rr) - 3m^6np(q - r) + 3m^5nnpp - mn^6(q + r)^2,$$
$$\begin{aligned} y = -m^6n(2qq - 2qr - rr) + 6m^5nnpq - 3m^4n^3pp + 3m^3n^4q(q + r) \\ - 3mmn^5p(q + r) - n^7(q + r)^2, \end{aligned}$$
$$\begin{aligned} z = +m^6n(-qq - 2qr + 2rr) + 6m^5nnpr + 3m^4n^3pp + 3m^3n^4r(q + r) \\ + 3mmn^5p(q + r) + n^7(q + r)^2, \end{aligned}$$

quorum cuborum summa iterum est cubus radicem habens v, ut sit

$$\begin{aligned} v = m^7(qq - qr + rr) - 3m^6np(q - r) + 3m^5nnpp - 3m^4n^3(qq - rr) \\ + 6m^3n^4p(q + r) + 2mn^6(q + r)^2. \end{aligned}$$

Hi vero numeri etiam sequenti modo exhiberi possunt:

$$\begin{array}{rcccccc} x = & +3m^5n^2pp & -3m^6npq & +3m^6npr & +m^7qq & -m^7qr & +m^7rr, \\ & & & & -mn^6 & -2mn^6 & -mn^6 \end{array}$$

$$\begin{array}{rcccccc} y = & -3m^4n^3pp & +6m^5n^2pq & -3m^2n^5pr & -2m^6nqq & +2m^6nqr & +m^6nrr, \\ & & -3m^2n^5 & & +3m^3n^4 & +3m^3n^4 & -n^7 \\ & & & & -n^7 & -2n^7 & \end{array}$$

$$\begin{array}{rcccccc} z = & +3m^4n^3pp & +3m^2n^5pq & +6m^5n^2pr & -m^6nqq & -2m^6nqr & +2m^6nrr, \\ & & & +3m^2n^5 & +n^7 & +3m^3n^4 & +3m^3n^4 \\ & & & & & +2n^7 & +n^7 \end{array}$$

$$\begin{array}{rcccccc} v = & +3m^5n^2pp & -3m^6npq & +3m^6npr & +m^7qq & -m^7qr & +m^7rr. \\ & & +6m^3n^4 & +6m^3n^4 & -3m^4n^3 & +4mn^6 & +3m^4n^3 \\ & & & & +2mn^6 & & +2mn^6 \end{array}$$

Quibus valoribus substitutis actu fit

$$x^3 + y^3 + z^3 = v^3.$$

15. Si singuli hi numeri insuper per coefficientem indefinitum multiplicentur, hae formulae continebunt sex litteras ab arbitrio nostro pendentes, quae quidem ad quatuor reducentur, unde eae latissime patere omnesque omnino casus in se complecti videntur; verumtamen ex ipsa solutione, qua ipsi v valorem a litteris x, y et z pendentem tribuimus, perspicitur has formulas nonnisi pro particularibus haberi posse. Ceterum quoque per alias positiones aliae eruuntur solutiones, quae pro certis casibus magis sint futurae idoneae; tum etiam methodus habetur ex inventa solutione quacunque particulari alias solutiones particulares eliciendi. His tamen omnibus artificiis, nisi in infinitum reiterentur, nulla solutio, quae pro generali haberi queat, obtineri potest. Quin etiam in universum fere adhuc est creditum huius

generis problemata natura sua ita esse comparata, ut solutionem generalem prorsus non admittant, ex quo sequens istius problematis solutio, quae revera est generalis, imprimis notatu digna et finibus Analyseos DIOPHANTEAE promovendis apta videtur.

PROBLEMA

16. *Invenire generatim omnes cuborum terniones, quorum summa sit cubus.*

SOLUTIO

Sint A, B, C radices ternorum cuborum et D radix cubica summae eorum, ita ut sit

$$A^3 + B^3 + C^3 = D^3,$$

cui aequationi haec forma tribuatur

$$A^3 + B^3 = D^3 - C^3.$$

Ponatur iam

$$A = p + q, \quad B = p - q, \quad C = r - s \quad \text{et } D = r + s,$$

qua positione amplitudo solutionis neutiquam restringitur. Hinc autem fit

$$A^3 + B^3 = 2p^3 + 6pqq \quad \text{et } D^3 - C^3 = 2s^3 + 6rrs$$

sicque erit

$$p(pp + 3qq) = s(ss + 3rr),$$

quae aequatio subsistere nequit, nisi $pp + 3qq$ et $ss + 3rr$ communem habeant divisorem. Constat autem tales numeros alios non habere divisores, nisi qui eiusdem sint formae;[1]) quod ut obtineatur, loco quatuor litterarum p, q, r et s aliae sex novae introducantur hoc modo

$$p = ax + 3by, \qquad s = 3cy - dx,$$
$$q = bx - ay, \qquad r = dy + cx,$$

1) Vide Commentationem 272 huius voluminis, prop. 7. F. R.

unde multo minus amplitudini solutionis vis infertur. Hinc autem erit

$$pp + 3qq = (aa + 3bb)(xx + 3yy)$$

et

$$ss + 3rr = (dd + 3cc)(xx + 3yy)$$

ac nostra aequatio per $xx + 3yy$ divisa induet sequentem formam

$$(ax + 3by)(aa + 3bb) = (3cy - dx)(dd + 3cc),$$

qua id iam sumus consecuti, ut litterae x et y unicam tantum obtineant dimensionem ideoque rationaliter definiri queant. Cum enim sit

$$\frac{x}{y} = \frac{-3b(aa + 3bb) + 3c(dd + 3cc)}{a(aa + 3bb) + d(dd + 3cc)},$$

ponatur

$$x = -3nb(aa + 3bb) + 3nc(dd + 3cc),$$
$$y = na(aa + 3bb) + nd(dd + 3cc).$$

Ex quibus valoribus litterae p, q, r, s ita definiuntur, ut sit

$$p = 3n(ac + bd)(dd + 3cc),$$
$$q = n(3bc - ad)(dd + 3cc) - n(aa + 3bb)^2,$$
$$r = n(dd + 3cc)^2 - n(3bc - ad)(aa + 3bb),$$
$$s = 3n(ac + bd)(aa + 3bb).$$

Atque hinc tandem radices cuborum quaesitorum A, B, C, D erunt

$$A = n(3ac + 3bc - ad + 3bd)(dd + 3cc) - n(aa + 3bb)^2,$$
$$B = n(3ac - 3bc + ad + 3bd)(dd + 3cc) + n(aa + 3bb)^2,$$
$$C = n(dd + 3cc)^2 - n(3ac + 3bc - ad + 3bd)(aa + 3bb),$$
$$D = n(dd + 3cc)^2 + n(3ac - 3bc + ad + 3bd)(aa + 3bb),$$

quibus valoribus obtinetur, ut sit

$$A^3 + B^3 + C^3 = D^3;$$

et cum solutio nulla restrictione sit limitata, utique latissime patet omnesque cuborum terniones complectitur, quorum summa iterum est cubus.

COROLLARIUM 1

17. Derivemus hinc formulas magis speciales ac primo quidem sit $d=0$ eritque

$$A = 9n(a+b)c^3 - n(aa+3bb)^2,$$
$$B = 9n(a-b)c^3 + n(aa+3bb)^2,$$
$$C = 9nc^4 - 3nc(a+b)(aa+3bb),$$
$$D = 9nc^4 + 3nc(a-b)(aa+3bb).$$

Si hic ulterius ponatur $b=a$, fiet

$$A = 18nac^3 - 16na^4, \quad B = 16na^4, \quad C = 9nc^4 - 24na^3c$$

et

$$D = 9nc^4;$$

sin autem fiat $b=-a$, eruetur

$$A = -16na^4, \quad B = 18nac^3 + 16na^4, \quad C = 9nc^4$$

et

$$D = 9nc^4 + 24na^3c.$$

COROLLARIUM 2

18. Ponamus nunc $c=0$ eritque

$$A = n(3b-a)d^3 - n(aa+3bb)^2,$$
$$B = n(3b+a)d^3 + n(aa+3bb)^2,$$
$$C = nd^4 - nd(3b-a)(aa+3bb),$$
$$D = nd^4 + nd(3b+a)(aa+3bb).$$

Si ulterius ponatur $b=a$, erit

$$A = 2nad^3 - 16na^4, \quad B = 4nad^3 + 16na^4, \quad C = nd^4 - 8na^3d,$$
$$D = nd^4 + 16na^3d;$$

sin autem fiat $a=-b$, erit

$$A = 4nbd^3 - 16nb^4, \quad B = 2nbd^3 + 16nb^4, \quad C = nd^4 - 16nb^3d,$$
$$D = nd^4 + 8nb^3d.$$

COROLLARIUM 3

19. Sit nunc $b = 0$ formulaeque nostrae fient

$$A = na(3c - d)(dd + 3cc) - na^4,$$
$$B = na(3c + d)(dd + 3cc) + na^4,$$
$$C = n(dd + 3cc)^2 - na^3(3c - d),$$
$$D = n(dd + 3cc)^2 + na^3(3c + d).$$

Quodsi iam praeterea statuatur $d = c$, erit

$$A = 8nac^3 - na^4, \quad B = 16nac^3 + na^4, \quad C = 16nc^4 - 2na^3c,$$
$$D = 16nc^4 + 4na^3c;$$

sin autem fiat $d = -c$, erit

$$A = 16nac^3 - na^4, \quad B = 8nac^3 + na^4, \quad C = 16nc^4 - 4na^3c,$$
$$D = 16nc^4 + 2na^3c.$$

COROLLARIUM 4

20. Ponatur denique $a = 0$ atque obtinebimus

$$A = 3nb(c + d)(dd + 3cc) - 9nb^4,$$
$$B = 3nb(d - c)(dd + 3cc) + 9nb^4,$$
$$C = n(dd + 3cc)^2 - 9nb^3(c + d),$$
$$D = n(dd + 3cc)^2 + 9nb^3(d - c).$$

Si ulterius ponatur $d = c$, erit

$$A = 24nbc^3 - 9nb^4, \quad B = 9nb^4, \quad C = 16nc^4 - 18nb^3c,$$
$$D = 16nc^4;$$

sin autem sit $c = -d$, habebitur

$$A = -9nb^4, \quad B = 24nbd^3 + 9nb^4, \quad C = 16nd^4,$$
$$D = 16nd^4 + 18nb^3d.$$

COROLLARIUM 5

21. Si numerorum A, B, C unus fiat negativus, quod pro lubitu effici potest, veluti si fiat $A = -E$, erit $B^3 + C^3 = D^3 + E^3$ sicque simul hoc problema generalissime dedimus solutum, quo bina cuborum paria quaeruntur, quorum summae sint inter se aequales. Sin autem duae radices prodeant negativae, veluti $A = -E$ et $B = -F$, erit $C^3 = D^3 + E^3 + F^3$ sicque denuo nostri problematis solutio habebitur.

SCHOLION 1

22. Formulae specialissimae in his corollariis exhibitae ad binas has reducuntur, siquidem in Corollario 3 pro a scribatur $2a$ et $n = \frac{n}{16}$, et in Corollario 1 $\frac{1}{2}a$ pro a:

$$A = nac^3 - na^4, \qquad A = 9nac^3 - na^4,$$
$$B = 2nac^3 + na^4, \qquad B = na^4,$$
$$C = nc^4 - na^3c, \qquad C = 9nc^4 - 3na^3c,$$
$$D = nc^4 + 2na^3c, \qquad D = 9nc^4,$$

quarum prior convenit cum supra (§ 8) inventa; altera autem praebet hunc casum simplicissimum $A = 8$, $B = 1$, $C = 6$ et $D = 9$, ita ut sit

$$1^3 + 6^3 + 8^3 = 9^3.$$

SCHOLION 2

23. Primo intuitu formulae generales in problemate erutae non latius patere videntur quam formulae supra (§ 14) exhibitae, cum utrinque quinque insint litterae arbitrariae atque istae insuper coefficientem communem recipere queant, ita ut etiam magis generales videantur. Interim tamen ipsa solutionis ratio declarat formulas in problemate inventas esse amplissimas, dum superiores insigni restrictione sunt limitatae. Quae restrictio quo clarius perspiciatur, ex § 13 perpendatur positio

$$v = mt + \frac{mmp + nn(q+r)}{mm}u = mt + pu + \frac{nn}{mm}(q+r)u.$$

Iam vero est $mt + pu = x$ et $y + z = (q + r)u$, ita ut positio sit

$$v = x + \frac{nn}{mm}(y + z).$$

Quare, ut fiat $x^3 + y^3 + z^3 = v^3$, in illa solutione assumitur esse

$$\frac{v - x}{y + z} = \frac{nn}{mm} = \text{quadrato};$$

sicque illa ad alios casus non pateat, nisi in quibus sit $\frac{v - x}{y + z}$ seu $\frac{D - A}{B + C}$ numerus quadratus. Quoties igitur $\frac{D - A}{B + C}$ non sit quadratum, casus in superioribus formulis non continetur; huiusmodi autem casus dari vel ex exemplo $1^3 + 6^3 + 8^3 = 9^3$ liquet, in quo neque $\frac{9 - 1}{6 + 8}$ neque $\frac{9 - 6}{1 + 8}$ neque $\frac{9 - 8}{1 + 6}$ fit quadratum. Solutio autem problematis tali restrictione non limitatur, cum sit

$$\frac{D - C}{A + B} = \frac{s}{p} = \frac{pp + 3qq}{ss + 3rr} = \frac{aa + 3bb}{dd + 3cc},$$

unde ex solutione generali ii tantum casus, quibus $\frac{aa + 3bb}{dd + 3cc}$ est numerus quadratus, in formulis superioribus § 14 continentur; ex quo summa generalitas nostrae solutionis manifesto elucet.

SCHOLION 3

24. Natura autem huius problematis numeros integros tantum postulat et quidem tales, qui sint primi inter se; si enim fuerit $A^3 + B^3 + C^3 = D^3$, tum problemati quoque satisfacient omnia tam aeque multipla quam aeque submultipla numerorum A, B, C, D; ideoque sufficiet eos tantum notasse casus, quibus numeri A, B, C, D fiunt cum integri tum primi inter se. Hunc in finem sumtis pro a, b, c, d numeris quibuscunque sive affirmativis sive negativis inde primum formentur

$$x = 3n(c(dd + 3cc) - b(aa + 3bb)),$$
$$y = n(d(dd + 3cc) + a(aa + 3bb))$$

ac pro n talis sumatur fractio, ut x et y fiant integri et primi inter se. Ex his porro formentur

$$p = ax + 3by, \quad q = bx - ay, \quad r = dy + cx \quad \text{et} \quad s = 3cy - dx,$$

qui denuo per communem divisorem, si quem habent, deprimantur. Hinc denique habebitur

$$A = p + q, \quad B = p - q, \quad C = r - s \quad \text{et} \quad D = r + s$$

sicque fiet

$$A^3 + B^3 + C^3 = D^3.$$

Atque casus, quibus unus horum numerorum fit negativus, simul omnes solutiones praebebunt, quibus summa duorum cuborum aequalis est summae duorum aliorum cuborum.

In hoc calculo conveniet copiam numerorum formae $mm + 3nn$ in promtu habere, unde deinceps formulae $aa + 3bb$ et $dd + 3cc$ desumi queant.[1]

1) In editione principe tabula sequens nonnullos errores continet, qui omnes fere etiam in *Comment. arithm.* inveniuntur, hac in editione autem correcti sunt. F. R.

Tabula numerorum formae $mm + 3nn$

Numerus n

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	0	3	12	27	48	75	108	147	192	243	300	363	432	507	588	675	768	867	972
1	1	4	13	28	49	76	109	148	193	244	301	364	433	508	589	676	769	868	973
2	4	7	16	31	52	79	112	151	196	247	304	367	436	511	592	679	772	871	976
3	9	12	21	36	57	84	117	156	201	252	309	372	441	516	597	684	777	876	981
4	16	19	28	43	64	91	124	163	208	259	316	379	448	523	604	691	784	883	988
5	25	28	37	52	73	100	133	172	217	268	325	388	457	532	613	700	793	892	997
6	36	39	48	63	84	111	144	183	228	279	336	399	468	543	624	711	804	903	
7	49	52	61	76	97	124	157	196	241	292	349	412	481	556	637	724	817	916	
8	64	67	76	91	112	139	172	211	256	307	364	427	496	571	652	739	832	931	
9	81	84	93	108	129	156	189	228	273	324	381	444	513	588	669	756	849	948	
10	100	103	112	127	148	175	208	247	292	343	400	463	532	607	688	775	868	967	
11	121	124	133	148	169	196	229	268	313	364	421	484	553	628	709	796	889	988	
12	144	147	156	171	192	219	252	291	336	387	444	507	576	651	732	819	912		
13	169	172	181	196	217	244	277	316	361	412	469	532	601	676	757	844	937		
14	196	199	208	223	244	271	304	343	388	439	496	559	628	703	784	871	964		
15	225	228	237	252	273	300	333	372	417	468	525	588	657	732	813	900	993		
16	256	259	268	283	304	331	364	403	448	499	556	619	688	763	844	931			
17	289	292	301	316	337	364	397	436	481	532	589	652	721	796	877	964			
18	324	327	336	351	372	399	432	471	516	567	624	687	756	831	912	999			
19	361	364	373	388	409	436	469	508	553	604	661	724	793	868	919				
20	400	403	412	427	448	475	508	547	592	643	700	763	832	907	988				
21	441	444	453	468	489	516	549	588	633	684	741	804	873	948					
22	484	487	496	511	532	559	592	631	676	727	784	847	916	991					
23	529	532	541	556	577	604	637	676	721	772	829	892	961						
24	576	579	588	603	624	651	684	723	768	819	876	939							
25	625	628	637	652	673	700	733	772	817	868	925	988							
26	676	679	688	703	724	751	784	823	868	919	976								
27	729	732	741	756	777	804	837	876	921	972									
28	784	787	796	811	832	859	892	931	976										
29	841	844	853	868	889	916	949	988											
30	900	903	912	927	948	975													
31	961	964	973	988															

SCHOLION 4

25. Ex hac tabula iam pro lubitu numeri pro $aa+3bb$ et $dd+3cc$ assumi poterunt, unde valores litterarum a, b, c, d habebuntur, quos tam affirmative quam negative accipere licet. Quodsi vero minores numeri pro A, B, C, D desiderentur, conveniet pro $aa+3bb$ et $3cc+dd$ eiusmodi valores capi, qui communem habeant divisorem. Statuatur ergo

$$aa+3bb=mk \quad \text{et} \quad dd+3cc=nk.$$

Tum vero sit

$$ac+bd=f \quad \text{et} \quad 3bc-ad=g$$

hincque fiet

$$A=n(3f+g)-mmk,$$
$$B=n(3f-g)+mmk,$$
$$C=nnk-m(3f+g),$$
$$D=nnk+m(3f-g),$$

ubi notandum est, quicunque valores pro f et g fuerint inventi, eos tam affirmative quam negative capi posse ob numeros a, b, c, d ambiguos; unde pro quovis casu sequentes habebuntur determinationes

$$\text{vel} \quad f=\pm(ac+bd), \quad g=\pm(3bc-ad)$$
$$\text{vel} \quad f=\pm(ac-bd), \quad g=\pm(3bc+ad).$$

Patet autem, si manente g capiatur f negative, eosdem numeros esse proditūros ordine tantum permutato, unde sufficit pro f valores tantum affirmativos assumsisse. Praeterea manifestum est, si sit $m=n$ seu

$$aa+3bb=dd+3cc,$$

tum fore $A=-C$ et $D=B$, unde et hos casus excludi oportebit. Denique si $f=0$, fit $A=-B$ et $C=D$[1]); qui propterea casus quoque sunt omittendi. Saepenumero quoque evenit, ut vel pro a et b vel pro c et d vel pro utrisque plures valores oriantur, ex quibus solutionum numerus eo maior evadit.

---

1) Editio princeps (atque etiam *Comment. arithm.*): $C=-D$. Correxit F. R.

EXEMPLUM 1

26. Capiatur $aa + 3bb = 19$, erit $a = 4$ et $b = 1$, tum vero $dd + 3ee = 76$ eritque

$$\text{vel} \quad d = 1, \quad e = 5$$
$$\text{vel} \quad d = 7, \quad e = 3$$
$$\text{vel} \quad d = 8, \quad e = 2.$$

Tum vero fit $m = 1$, $n = 4$ et $k = 19$. Pro f autem et g sequentes prodibunt valores

$$\text{I. } f = 21, \; g = \pm 11, \qquad \text{II. } f = 19, \; g = \pm 19, \qquad \text{III. } f = 19, \; g = \pm 19,$$
$$\text{IV. } f = 5, \; g = \pm 37, \qquad \text{V. } f = 16, \; g = \pm 26, \qquad \text{VI. } f = 0, \; g = \pm 38,$$

unde tertius casus et sextus sunt excludendi. Atque hinc erit

$$A = 12f + 4g - 19,$$
$$B = 12f - 4g + 19,$$
$$C = 304 - 3f - g,$$
$$D = 304 + 3f - g.$$

Hinc ergo reperietur pro valore primo $f = 21$ et $g = \pm 11$

$$A = 233 \pm 44,$$
$$B = 271 \mp 44,$$
$$C = 241 \mp 11,$$
$$D = 367 \mp 11,$$

ergo

pro signis superioribus	pro signis inferioribus		
$A = 277,$	$A = 189,$	seu	$A = 3,$
$B = 227,$	$B = 315,$		$B = 5,$
$C = 230,$	$C = 252,$		$C = 4,$
$D = 356,$	$D = 378$		$D = 6.$

Casus autem II et III dividendo formulas per 19 ob $f = 1 \cdot 19$ et $g = \pm 1 \cdot 19$ dabunt

$$A = 11 \pm 4,$$
$$B = 13 \mp 4,$$
$$C = 13 \mp 1,$$
$$D = 19 \mp 1,$$

ergo

			vel		vel
$A = 15,$	seu	$A = 5,$		$A = 7,$	
$B = 9,$		$B = 3,$		$B = 17,$	
$C = 12,$		$C = 4,$		$C = 14,$	
$D = 18$		$D = 6,$		$D = 20.$	

Casus IV, quo $f = 5$ et $g = \pm 37$, dat

$$A = 41 \pm 148,$$
$$B = 79 \mp 148,$$
$$C = 289 \mp 37,$$
$$D = 319 \mp 37,$$

ergo

			vel		vel
$A = 189,$	seu	$A = 63,$		$A = -107,$	
$B = -69,$		$B = -23,$		$B = 227,$	
$C = 252,$		$C = 84,$		$C = 326,$	
$D = 282$		$D = 94,$		$D = 356.$	

Casus V, quo $f = 16$ et $g = \pm 26$, dat

$$A = 173 \pm 104,$$
$$B = 211 \mp 104,$$
$$C = 256 \mp 26,$$
$$D = 352 \mp 26,$$

ergo

vel	vel	seu
$A = 277,$	$A = 63,$	$A = 23,$
$B = 107,$	$B = 315,$	$B = 105,$
$C = 230,$	$C = 282,$	$C = 94,$
$D = 326,$	$D = 378$	$D = 126.$

En ergo plures cuborum terniones ex unica positione inventos:

$$227^3 + 230^3 + 277^3 = 356^3, \qquad 107^3 + 356^3 = 227^3 + 326^3,$$
$$107^3 + 230^3 + 277^3 = 326^3, \qquad 23^3 + 94^3 = 63^3 + 84^3,$$
$$23^3 + 94^3 + 105^3 = 126^3,$$
$$7^3 + 14^3 + 17^3 = 20^3,$$
$$3^3 + 4^3 + 5^3 = 6^3,$$

unde colligitur

$$356^3 - 227^3 = 230^3 + 277^3 = 326^3 - 107^3,$$

item

$$126^3 - 105^3 = 63^3 + 84^3 = 23^3 + 94^3.$$

EXEMPLUM 2

27. Sit $aa + 3bb = 28$; erit

$$\text{vel} \quad a = 1, \quad b = 3$$
$$\text{vel} \quad a = 4, \quad b = 2$$
$$\text{vel} \quad a = 5, \quad b = 1;$$

tum vero sit $dd + 3cc = 84$; erit

$$\text{vel} \quad d = 3, \quad c = 5$$
$$\text{vel} \quad d = 6, \quad c = 4$$
$$\text{vel} \quad d = 9, \quad c = 1$$

hincque $k = 28$, $m = 1$ et $n = 3$; tum vero pro f et g sequentes prodibunt valores

$$\text{I. } f=14,\ g=\pm 42,\quad \text{II. } f=4,\ g=\pm 48,\quad \text{III. } f=22,\ g=\pm 30,$$
$$\text{IV. } f=14,\ g=\pm 42,\quad \text{V. } f=28,\ g=\pm 0,\quad \text{VI. } f=26,\ g=\pm 18,$$

ubi notandum est hos valores, quorum I et IV conveniunt, oriri ex sola positione $a=1$ et $b=3$ et reliquas duas eosdem producere. Hinc ergo habebimus

$$\begin{aligned} A &= 9f+3g-28, \\ B &= 9f-3g+28, \\ C &= 252-3f-g, \\ D &= 252+3f-g, \end{aligned}$$

unde casus primus et quartus dabunt per 14 dividendo

$$\begin{aligned} A &= 7\pm 9, \\ B &= 11\mp 9, \\ C &= 15\mp 3, \\ D &= 21\mp 3, \end{aligned}$$

ergo

$$\begin{array}{lcl} \text{vel} & & \text{vel} \\ A=16=8, & & A=-2=-1, \\ B=2=1, & & B=20=10, \\ C=12=6, & & C=18=9, \\ D=18=9, & & D=24=12. \end{array}$$

Casus vero secundus per 4 dividendo dat

$$\begin{aligned} A &= 2\pm 36, \\ B &= 16\mp 36, \\ C &= 60\mp 12, \\ D &= 66\mp 12, \end{aligned}$$

ergo

$$\begin{array}{lcl} \text{vel} & & \text{vel} \\ A=38=19, & & A=-34=-17, \\ B=-20=-10, & & B=52=26, \\ C=48=24, & & C=72=36, \\ D=54=27, & & D=78=39. \end{array}$$

Casus tertius per 2 divisus dat

$$A = 85 \pm 45,$$
$$B = 113 \pm 45,$$
$$C = 93 \pm 15,$$
$$D = 159 \pm 15,$$

ergo

vel	vel
$A = 130 = 65,$	$A = 40 = 20,$
$B = 68 = 34,$	$B = 158 = 79,$
$C = 78 = 39,$	$C = 108 = 54,$
$D = 144 = 72,$	$D = 174 = 87.$

Casus quintus dat per 28 divisus

$$A = 8 = 4,$$
$$B = 10 = 5,$$
$$C = 6 = 3,$$
$$D = 12 = 6.$$

Casus denique sextus per 2 divisus dat

$$A = 103 \pm 27,$$
$$B = 131 \pm 27,$$
$$C = 87 \pm 9,$$
$$D = 165 \pm 9,$$

ergo

vel	vel
$A = 130 = 65 = 5,$	$A = 76 = 38,$
$B = 104 = 52 = 4,$	$B = 158 = 79,$
$C = 78 = 39 = 3,$	$C = 96 = 48,$
$D = 156 = 78 = 6,$	$D = 174 = 87.$

Ex hoc ergo exemplo sequentes resultant formulae:

$$1^3 + 6^3 + 8^3 = 9^3, \quad \text{et} \quad 1^3 + 12^3 = 9^3 + 10^3,$$
$$34^3 + 39^3 + 65^3 = 72^3, \qquad 10^3 + 27^3 = 19^3 + 24^3,$$
$$20^3 + 54^3 + 79^3 = 87^3, \qquad 17^3 + 39^3 = 26^3 + 36^3,$$
$$3^3 + 4^3 + 5^3 = 6^3,$$
$$38^3 + 48^3 + 79^3 = 87^3$$

hincque sequitur

$$87^3 - 79^3 = 20^3 + 54^3 = 38^3 + 48^3.$$

Patet ergo ex quovis exemplo assumto plures huiusmodi formulas obtineri, inter quas autem eaedem saepius recurrent; quemadmodum casus

$$3^3 + 4^3 + 5^3 = 6^3$$

in hoc exemplo et praecedente bis occurrit.

28. En ergo solutionem generalem problematis, quo quaeruntur quatuor numeri rationales A, B, C, D, ita ut sit $A^3 + B^3 + C^3 = D^3$, seu, quod eodem redit, quo quaeruntur quatuor numeri rationales p, q, r et s, ut sit

$$p(pp + 3qq) = s(ss + 3rr).$$

Quae problemata cum methodis solitis nonnisi particulariter resolvi queant, manifestum est has methodos solitas adhuc insigni defectu laborare ideoque notabilem adhuc perfectionem desiderare. Tum vero, quod hic de unico problemate ostendimus, nullum est dubium, quin id in infinitis aliis pari successu praestari possit. In genere quidem patet simili modo huiusmodi aequationem

$$\alpha p(mpp + nqq) = \beta s(mss + nrr)$$

vel etiam hanc latius patentem

$$(\alpha p + \beta q + \gamma r + \delta s + \varepsilon)(mpp + nqq) = (ap + bq + cr + ds + e)(mrr + nss)$$

rationaliter generalissime resolvi posse ponendo

$$p = nfx + gy, \qquad q = mfy - gx$$

et

$$r = nhx + ky, \qquad s = mhy - kx;$$

fiet enim

$$mpp + nqq = (gg + mnff)(nxx + myy)$$

et

$$mrr + nss = (kk + mnhh)(nxx + myy),$$

unde aequatio divisa per $nxx + myy$ continebit incognitas x et y unius tantum dimensionis, ex qua propterea sine ulla restrictione earum valores rationaliter determinabuntur.

29. Non immerito igitur suspicari licet et aliorum problematum DIOPHANTEORUM, quorum adhuc nonnisi solutiones particulares sunt repertae, solutiones quoque generales dari neque discrimen supra memoratum ex solutionum generalitate et particularitate petitum esse essentiale; unde patet, quanta adhuc incrementa in Analysi DIOPHANTEA desiderentur. Ad quae si unquam penetrare contigerit, nullum est dubium, quin inde universa Analysis tam finitorum quam infinitorum haud contemnenda subsidia sit acceptura. Cum enim in calculo integrali praecipuum artificium in hoc versetur, ut formulae differentiales irrationales in rationales transformentur, hoc artificium ipsum uti ex Analysi DIOPHANTEA in hunc calculum est translatum, ita etiam indidem maiora auxilia merito expectantur; ex quo studium, quod in ista Analysi, utcunque sterilis alias in se spectata videatur, amplificanda impenditur, neutiquam inutiliter collocari est censendum.

30. Hic porro alia conditio non minus attentione digna notari meretur, quod saepius in Analysi DIOPHANTEA eiusmodi problemata occurrunt, quae per methodos consuetas solutionem generalem admittere videntur, cum tamen haec solutio tantum sit particularis; quibus casibus peculiaria artificia adhiberi debent, ut restrictio, qua methodus consueta est limitata, tollatur. Veluti si duo cubi in numeris integris quaerantur, quorum summa sit numerus quadratus, solutio nullo modo restricta obtineri videtur, si ista aequatio

$$x^3 + y^3 = zz$$

ita resolvatur, ut ponatur

$$x = \frac{pz}{r} \quad \text{et} \quad y = \frac{qz}{r}.$$

Fiet enim $(p^3 + q^3)z = r^3$ ideoque

$$z = \frac{r^3}{p^3 + q^3}$$

et

$$x = \frac{prr}{p^3 + q^3}, \quad y = \frac{qrr}{p^3 + q^3}.$$

Unde ut x et y fiant numeri integri, statuatur $r = n(p^3 + q^3)$, ut habeatur

$$x = nnp(p^3 + q^3) \text{ et } y = nnq(p^3 + q^3),$$

eritque

$$x^3 + y^3 = n^6(p^3 + q^3)^4 = \text{quadrato}.$$

31. Etsi autem ista solutio generalis videtur, tamen nulli alii numeri pro x et y inveniuntur, nisi qui communem habent factorem $p^3 + q^3$, ita ut hinc concludendum videatur nullos dari numeros inter se primos, qui pro x et y substituti quaestioni satisfaciant. Interim tamen casu, quo $x = 1$ et $y = 2$, perspicuum est fore $x^3 + y^3 = 9 =$ quadrato. Tametsi autem hic casus ex formulis nostris derivari potest ponendo $p = 1$, $q = 2$ et $n = \frac{1}{3}$, unde utique prodit $x = \frac{1}{9} \cdot 9 = 1$ et $y = \frac{2}{9} \cdot 9 = 2$, tamen, ut hinc alii huius generis casus eliciantur, necesse est, ut pro p et q eiusmodi numeri accipiantur, quorum cuborum summa sit quadratum, puta $= ss$, ut deinceps poni possit $n = \frac{1}{s}$, unde prodibit $x = p$ et $y = q$; quo pacto id ipsum, quod hic quaeritur, iam tanquam cognitum postulatur, ut scilicet duo cubi assignari queant, quorum summa sit quadratum. Quemadmodum ergo huic incommodo sit occurrendum, in sequenti problemate videamus.

PROBLEMA

32. *Invenire duos numeros integros inter se primos, quorum cubi additi faciant quadratum.*

SOLUTIO

Sint x et y numeri quaesiti, ita ut esse debeat

$$x^3 + y^3 = \text{quadrato}.$$

Debet ergo [esse] $(x + y)(xx - xy + yy) =$ quadrato. At de his duobus factoribus annoto eos esse vel primos inter se vel ternarium pro communi mensura

admittere, unde solutio fiet bipartita, quae autem ita in unam compingetur, ut uterque factor seorsim $x+y$ et $xx-xy+yy$ vel quadratum esse debeat vel triplum quadratum.

I. Sit primum uterque factor quadratus ac ponatur

$$xx-xy+yy=(pp-pq+qq)^2$$

eritque vel

$$x=pp-2pq \quad \text{et} \quad y=pp-qq$$

vel

$$x=2pq-pp \quad \text{et} \quad y=qq-pp.$$

Priori casu ergo oportet, ut sit $x+y=2pp-2pq-qq$ quadratum. Quae forma cum sit $=3pp-(p+q)^2$, si ponatur $=rr$, oporteret esse $3pp=(p+q)^2+rr=$ summae duorum quadratorum, quod est impossibile. Relinquitur ergo alter casus, quo

$$x+y=qq+2pq-2pp=(q+p)^2-3pp=\text{quadrato},$$

cui satisfit ponendo

$$p=2mn \quad \text{et} \quad q=3mm-2mn+nn,$$

$$x=2pq-pp=4mn(3mm-3mn+nn),$$

$$y=qq-pp=(3mm+nn)(3mm-4mn+nn)=(m-n)(3m-n)(3mm+nn).$$

II. Tum vero ponatur

$$xx-xy+yy=\text{triplo quadrato}=3(pp-pq+qq)^2,$$

cui triplici modo satisfit:

$$\begin{array}{lll} \text{I.} & x=2pp-2pq-qq, & y=pp+2pq-2qq, \\ \text{II.} & x=2pp-2pq-qq, & y=pp-4pq+qq, \\ \text{III.} & x=pp+2pq-2qq, & y=-pp+4pq-qq. \end{array}$$

Casu primo fit $x+y=3pp-3qq=$ triplo quadrato seu $pp-qq=$ quadrato, unde fit

$$p=mm+nn \quad \text{et} \quad q=2mn$$

ideoque

$$x=2(m^4-2m^3n-2mn^3+n^4),$$

$$y=m^4+4m^3n-6mmnn+4mn^3+n^4.$$

Casu secundo fit $x+y=3pp-6pq=$ triplo quadrato, ergo $pp-2pq=$ quadrato, cui satisfit ponendo

$$p=2mm \quad \text{et} \quad q=mn-nn,$$

unde oritur

$$x=\quad 3m^4+6mmnn-n^4,$$
$$y=-3m^4+6mmnn+n^4.$$

Casu denique tertio fit $x+y=6pq-3qq=3\square$ et $2pq-qq=\square$, unde fit

$$p=mm+nn \quad \text{et} \quad q=2mm$$

ideoque

$$x=-3m^4+6mmnn+n^4,$$
$$y=\quad 3m^4+6mmnn-n^4,$$

quae cum illis congruunt.

En ergo ternas solutiones problematis propositi:

$$\text{I.}\ \begin{cases} x= & 4mn(3mm-3mn+nn), \\ y= & (m-n)(3m-n)(3mm+nn), \end{cases}$$

$$\text{II.}\ \begin{cases} x= & 2(m^4-2m^3n-2mn^3+n^4), \\ y= & m^4+4m^3n-6mmnn+4mn^3+n^4, \end{cases}$$

$$\text{III.}\ \begin{cases} x= & 3m^4+6mmnn-n^4, \\ y= & -3m^4+6mmnn+n^4, \end{cases}$$

ubi quidem secunda forma in tertia, quae cum quarta convenit, contenta deprehenditur, ita ut secunda uti magis complicata omitti possit.

COROLLARIUM 1

33. Si hae formulae pro x et y inventae per numerum quadratum quemcunque multiplicentur, eae quaesito aeque satisfacient; ita scilicet summa cuborum x^3+y^3 fiat numerus quadratus, unde numeri quotcunque non primi inter se obtinebuntur. Simili autem modo si hae formulae communem habuerint divisorem quadratum, per eum divisae quaesito perinde satisfacient, unde numeri inter se primi pro x et y inveniuntur, quales hic proprie quaeruntur. Geminas ergo pro hoc negotio habebimus formulas:

$$\text{I.}\quad \begin{cases} x = 4mn(3mm - 3mn + nn), \\ y = (m - n)(3m - n)(3mm + nn), \end{cases}$$

$$\text{II.}\quad \begin{cases} x = 3m^4 + 6mmnn - n^4, \\ y = -3m^4 + 6mmnn + n^4. \end{cases}$$

COROLLARIUM 2

34. Evidens est dari infinitos casus, quibus altera harum formularum recipit valorem negativum; quod in prioribus evenit, si vel m sit negativum vel n, vel n contineatur intra limites m et $3m$, in posterioribus autem, si vel $\frac{nn}{mm}$ sit maius quam $3 + 2\sqrt{3}$ vel $\frac{nn}{mm}$ minus quam $2\sqrt{3} - 3$[1]. His ergo casibus duo reperiuntur cubi, quorum differentia est quadratum.

1) Editio princeps (atque etiam *Comment. arithm.*): *si vel* $\frac{nn}{mm}$ *sit maius, quam* $3(1 + \sqrt{2})$, *vel* $\frac{nn}{mm}$ *minus, quam* $3(\sqrt{2} - 1)$. Correxit F. R.

SPECIMEN DE USU OBSERVATIONUM IN MATHESI PURA

Commentatio 256 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 6 (1756/7), 1761, p. 185—230
Summarium ibidem p. 19—21

SUMMARIUM

Haud parum paradoxum videbitur etiam in Matheseos parte, quae pura vocari solet, multum observationibus tribui, quae vulgo nonnisi in obiectis externis sensus nostros afficientibus locum habere videntur. Cum igitur numeri per se unice ad intellectum purum referri debeant, quid observationes et quasi experimenta in eorum natura exploranda valeant, vix perspicere licet. Interim tamen hic solidissimis rationibus ostensum est plerasque numerorum proprietates, quas quidem adhuc agnovimus, primum per solas observationes nobis innotuisse, idque plerumque multo antequam veritatem earum rigidis demonstrationibus confirmaverimus. Quin etiam adhuc multae numerorum proprietates nobis sunt cognitae, quas tamen nondum demonstrare valemus; ad earum igitur cognitionem solis observationibus sumus perducti. Ex quo perspicuum est in scientia numerorum, quae etiamnunc maxime est imperfecta, plurimum ab observationibus esse expectandum, quippe quibus ad novas proprietates numerorum continuo deducimur, in quarum demonstratione deinceps sit elaborandum. Talis cognitio solis observationibus innixa, quamdiu quidem demonstratione destituitur, a veritate sollicite est discernenda atque ad inductionem referri solet. Non desunt autem exempla, quibus inductio sola in errores praecipitaverit. Quascunque ergo numerorum proprietates per observationes cognoverimus, quae idcirco sola inductione innituntur, probe quidem cavendum est, ne eas pro veris habeamus, sed ex hoc ipso occasionem nanciscimur eas accuratius explorandi earumque vel veritatem vel falsitatem ostendendi, quorum utrumque utilitate non caret.

Tali igitur instituto Cel. EULERUS omnes numeros ex quadrato et duplo alius quadrati compositos contemplatur, quibus ad 500 usque expositis plures insignes earum proprietates observat, veluti quod hi numeri, siquidem fuerint compositi, alios divisores non admittant, nisi qui ipsi sint eiusdem indolis, tum vero, si fuerint primi, eos semper multiplum octonarii vel unitate vel ternario superare. Hinc autem vicissim concludere licet omnes numeros primos vel unitate vel ternario multiplum octonarii superantes semper esse compositos ex quadrato et duplo quadrato seu in forma $aa + 2bb$ contineri; quae postrema observatio non solum in numeris minoribus ad 500 usque locum habet, sed inductionem longe ultra 1000 continuando nulla exceptio se prodidit. Etiamsi autem reliquas observationes omnes Auctori firmis demonstrationibus communire licuerit, in hac postrema tamen aqua ipsi haesit, neque tamen minus ea pro vera habenda videtur[1]; ex quo harum speculationum studiosis pulcerrima occasio suppeditatur vires suas in ea demonstranda exercendi. Demonstrationes autem huiusmodi arithmeticae geometricis longe praestant multoque maius ingenii acumen postulant; quare cum demonstrationes geometricae ad vim ingenii acuendam tantopere commendari solent, demonstrationes certe arithmeticae isto honore multo magis dignae sunt iudicandae eoque magis eos laudari oportet, qui in hoc genere demonstrationum operam suam collocant.

Inter tot insignes numerorum proprietates, quae adhuc sunt inventae ac demonstratae, nullum est dubium, quin pleraeque primum ab inventoribus tantum sunt observatae et in multiplici numerorum tractatione animadversae, antequam de iis demonstrandis cogitaverint. Ita de eo numerorum primorum ordine, qui unitate superant multiplum quaternarii, cuiusmodi sunt 5, 13, 17, 29, 37, 41 etc., ante sine dubio est observatum eorum singulos in duo quadrata secari posse, quam in eo elaboratum, ut huius observationis veritas per solidam demonstrationem evinceretur.[2]) Quod deinde quilibet numerus in quatuor vel pauciora quadrata distribui possit, DIOPHANTO iam notum fuisse videtur, nemo autem ante FERMATIUM est professus se huius veritatis demonstrationem habere, quam autem nusquam publice edidit, ita ut mea demonstratio, quam ante aliquod tempus concinnavi, pro prima, quae quidem publice fuerit proposita, sit habenda.[3]) Interim tamen fateri cogor demonstra-

1) Secundum manuscriptum; editio princeps: *in hac postrema tamen aquam ipsi haesisse confitetur, neque tamen minus eam pro vera habet.* F. R.

2) Vide Commentationes 228 et 241 huius voluminis. F. R.

3) Vide Commentationem 242 huius voluminis, imprimis § 65. F. R.

tionem FERMATIANAM, etiamsi mihi nihil omnino de principiis, quibus innitebatur, suspicari licuerit, mea multo fuisse perfectiorem ac longe latius patuisse. Asseverat enim FERMATIUS se ex eodem fonte aliorum quoque Theorematum demonstrationes hausisse, cuius generis sunt, quod omnis numerus integer sit summa trium pauciorumve numerorum trigonalium; item quod omnis numerus integer sit summa quinque vel pauciorum numerorum pentagonalium; item sex pauciorumve numerorum hexagonalium, et ita porro de reliquis numeris polygonalibus in infinitum.[1]) Ego vero etiamsi resolutionem cuiusque numeri in quatuor pauciorave quadrata demonstravi, tamen omnem adhuc operam in istis reliquis theorematibus demonstrandis inutiliter consumsi neque ullo modo etiamnunc saltem resolutionem in tres paucioresve trigonales ostendere potui, etiamsi ea simplicior videatur quam resolutio in quatuor pauciorave quadrata.[2])

Verum et has eximias numerorum proprietates FERMATIUS multo ante per inductionem conclusisse est putandus, quam eas demonstrare didicerit. Ex quibus merito colligimus in numerorum indole scrutanda observationi et inductioni, cui omnes has elegantissimas proprietates acceptas referre debemus, plurimum esse tribuendum ideoque ne nunc quidem ab hoc negotio ulterius prosequendo esse desistendum. Hoc enim modo pertingimus ad huiusmodi proprietatum cognitionem, quae alias nobis perpetuo ignotae mansissent, ac tum demum occasionem nanciscimur ad investigationem demonstrationum vires nostras intendendi; veritates namque pleraeque huius generis ita sunt comparatae, ut prius agnosci debeant, quam demonstrari possint. Quamvis autem huiusmodi proprietas per assiduam observationem fuerit animadversa, quae per se menti non parum est iucunda, tamen, nisi demonstratio solida accesserit, de eius veritate non satis certi esse possumus; exempla enim non desunt, quibus sola inductio in errorem praecipitaverit. Tum vero ipsa demonstratio non solum omnia dubia tollit, sed etiam naturae numerorum penetralia non mediocriter recludit nostramque numerorum cognitionem continuo magis promovet, a cuius certe doctrinae perfectione adhuc longissime sumus remoti. Verum si cui haec forte non magni momenti esse videantur, quod vix unquam ullum in Mathesi applicata usum habitura puten-

1) Vide notam 4 p. 358 F. R.

2) Vide etiam L. EULERI Commentationem 586 (indicis ENESTROEMIANI): *Considerationes super theoremate FERMATIANO de resolutione numerorum in numeros polygonales*, *Opuscula analytica* 2, 1785, p. 3; *LEONHARDI EULERI Opera omnia*, series I, vol. 4. F. R.

tur, usus, quem inde in ratiocinando adipiscimur, certe non est contemnendus. Sunt enim plerumque huius generis veritates ita reconditae, ut earum demonstrationes tam incredibilem circumspectionem quam eximiam ingenii vim requirant. Quare cum vulgo ad ratiocinii facultatem comparandam demonstrationes geometricae commendari soleant, quippe quae regularum ratiocinandi usum maxime contineant, nescio, annon ad hunc scopum demonstrationes arithmeticae multo magis sint accommodatae; in his enim multo maiori cura est cavendum, ne a praescriptis Logicorum regulis aberremus, quoniam plerumque nimis est difficile in errorem non prolabi. Deinde vero huius generis demonstrationes arithmeticae multo maiorem sollertiam et sagacitatem ingenii postulant quam geometricae; unde qui in his fuerit exercitatus, longe facilius errorem in ratiocinando usu edoctus evitabit sibique promtum ratiocinii usum multo certius comparabit. Atque ob haec tam insignia commoda perlustrationes naturae numerorum minime relinquendae videntur; in quibus ne inutiliter versemur, ab observationibus erit exordiendum hincque ad demonstrationem proprietatum observatarum progrediendum.

Huiusmodi operationem iam ante aliquot annos confeci[1]) in contemplatione divisorum cuiusque numeri, qui est summa duorum quadratorum; nunc igitur, ut viam ad alias numerorum proprietates cognoscendas sternam, contemplaturus sum numeros, qui ex quadrato et duplo quadrati sunt compositi, quales in hac forma generali $2aa+bb$ sunt contenti, atque in divisores horum numerorum sum inquisiturus. At hic quidem statim notari convenit radices horum duorum quadratorum numeros inter se primos esse oportere; alioquin enim quilibet numerus posset esse divisor, quadratum scilicet numeri, qui foret radicum communis divisor; quamobrem numeros a et b, ex quibus forma $2aa+bb$ componitur, inter se primos statuam.

CONSIDERATIO CIRCA NUMEROS IN HAC FORMA $2aa+bb$ CONTENTOS

Exponantur primo numeri in forma $2+bb$ contenti, tum numeri huius formae $8+bb$ exclusis numeris paribus pro b substituendis, tertio numeri formae $18+bb$ sumendo pro b numeros per 3 non divisibiles.

1) Vide Commentationem 228 huius voluminis. F. R.

quarto numeros formae $32 + bb$ sumendo pro b numeros per 2 non divisibiles, et ita porro. Sicque obtinebuntur sequentes numerorum progressiones:

$2 + bb$) 3, 6, 11, 18, 27, 38, 51, 66, 83, 102, 123, 146, 171, 198, 227, 258, 291, 326, 363, 402, 443, 486.

$8 + bb$) 9, 17, 33, 57, 89, 129, 177, 233, 297, 369, 449.

$18 + bb$) 19, 22, 34, 43, 67, 82, 118, 139, 187, 214, 274, 307, 379, 418.

$32 + bb$) 33, 41, 57, 81, 113, 153, 201, 257, 321, 393, 473.

$50 + bb$) 51, 54, 59, 66, 86, 99, 114, 131, 171, 194, 219, 246, 306, 339, 374, 411, 491.

$72 + bb$) 73, 97, 121, 193, 241, 361, 433.

$98 + bb$) 99, 102, 107, 114, 123, 134, 162, 179, 198, 219, 242, 267, 323, 354, 387, 422, 459, 498.

$128 + bb$) 129, 137, 153, 177, 209, 249, 297, 353, 417, 489.

$162 + bb$) 163, 166, 178, 187, 211, 226, 262, 283, 331, 358, 418, 451.

$200 + bb$) 201, 209, 249, 281, 321, 369, 489.

$242 + bb$) 243, 246, 251, 258, 267, 278, 291, 306, 323, 342, 386, 411, 438, 467, 498.

$288 + bb$) 289, 313, 337, 409, 457.

$338 + bb$) 339, 342, 347, 354, 363, 374, 387, 402, 419, 438, 459, 482.

$392 + bb$) 393, 401, 417, 473.

$450 + bb$) 451, 454, 466, 499.

OBSERVATIO 1

Excerpamus hinc numeros primos, ut nanciscamur omnes numeros primos formae $2aa + bb$, qui quidem 500 non superent, quippe ad quem terminum omnes progressiones praecedentes produximus, atque isti numeri primi reperientur esse

3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97, 107, 113, 131, 137, 139, 163, 179, 193, 211, 227, 233, 241, 251, 257, 281, 283, 307, 313, 331, 337, 347, 353, 379, 401, 409, 419, 433, 443, 449, 457, 467, 491, 499.

De his ergo observo singulos nonnisi semel in serie numerorum formae $2aa + bb$ occurrere, *ita ut numerus primus, qui fuerit aggregatum ex quadrato et duplo quadrato, sit unico modo huiusmodi aggregatum.*

OBSERVATIO 2

Si ex numeris expositis excerpantur ii, qui sunt producta ex binario et numero primo, illi in ordinem digesti erunt

6, 22, 34, 38, 82, 86, 118, 134, 146, 166, 178, 194, 214, 226, 262, 274, 278, 326, 358, 386, 422, 454, 466, 482,

ubi alii numeri non occurrunt nisi ipsi numeri primi formae $2aa + bb$ duplicati, ac singuli hi quidem numeri semel tantum reperiuntur.

Qui ergo numerus primus in forma $2aa + bb$ fuerit contentus, eius quoque duplum erit numerus formae $2aa + bb$, atque unico modo.

Ceterum cum a et b sint numeri inter se primi ideoque alter eorum certo impar, manifestum est nullos dari in forma $2aa + bb$ numeros per 4 divisibiles.

OBSERVATIO 3

Cum in numeris expositis alii sint impares, alii pares et quidem impariter pares, observo porro:

Si quis numerus impar inter illos numeros reperiatur, tum quoque eius duplum certo occurrere; ac vicissim quicunque numerus par in illis numeris occurrit, eius quoque semissis ibidem certo reperietur.

OBSERVATIO 4

Quodsi iam reliquos numeros non primos spectemus singulosque in suos factores primos resolvamus, unicuique autem in parenthesi adscribamus, quot vicibus occurrat, sequentes nanciscemur:

3^2 (1), 3^3 (1), $3 \cdot 11$ (2), $3 \cdot 17$ (2), $3 \cdot 19$ (2), 3^4 (1), $3^2 \cdot 11$ (2), 11^2 (1), $3 \cdot 41$ (2), $3 \cdot 43$ (2), $3^2 \cdot 17$ (2), $3^2 \cdot 19$ (2), $3 \cdot 59$ (2), $11 \cdot 17$ (2), $3 \cdot 67$ (2), $11 \cdot 19$ (2), $3 \cdot 73$ (2), 3^5 (1), $3 \cdot 83$ (2), $3 \cdot 89$ (2), 17^2 (1), $3 \cdot 97$ (2), $3^3 \cdot 11$ (2), $3 \cdot 107$ (2), $17 \cdot 19$ (2), $3 \cdot 113$ (2), 19^2 (1), $3 \cdot 11^2$ (2), $3^2 \cdot 41$ (2), $3^2 \cdot 43$ (2), $3 \cdot 131$ (2), $3 \cdot 137$ (2), $3 \cdot 139$ (2), $11 \cdot 41$ (2), $3^3 \cdot 17$ (2), $11 \cdot 43$ (2), $3 \cdot 163$ (2),

Hic iam observo omnia producta ex numeris primis formae $2aa+bb$ per quamcunque combinationem nata occurrere, *ita ut productum ex quotcunque numeris formae $2aa+bb$ semper sit numerus in quadratum et duplum quadratum resolubilis, ac plus quidem uno modo, si ex diversis factoribus fuerit conflatus.*

OBSERVATIO 5

Imprimis autem hic animadverto in his numeris compositis nullos alios factores primos occurrere, nisi qui ipsi sint formae $2aa+bb$, unde colligo per inductionem:

Omnes numeros formae $2aa+bb$, siquidem a et b sint numeri inter se primi, nullos alios divisores admittere primos, nisi qui ipsi sint huius formae $2aa+bb$.

Binarium quidem vidimus inter divisores occurrere posse, verum cum $2aa+bb$ casu $b=0$ et $a=1$ binarium praebeat, etiam ipsum binarium in forma $2aa+bb$ complecti licet.

OBSERVATIO 6

Cum ergo omnis numerus formae $2aa+bb$ existentibus a et b primis inter se alios divisores primos non admittat, nisi qui in serie numerorum in observatione prima exhibitorum contineantur, si ipsis quidem binarius adiungatur, circa istos numeros primos observo intra illos nullos numeros sive huius formae $8n-1$ sive huius $8n-3$ reperiri.

De numeris ergo primis formae $8n-1$ et $8n-3$ affirmare licet eos non solum non esse numeros formae $2aa+bb$, sed etiam ne divisores quidem esse posse ullius numeri formae $2aa+bb$, siquidem a et b sint primi inter se.

OBSERVATIO 7

Numeris ergo primis huius geminae formae $8n-1$ et $8n-3$ exclusis praeter binarium nulli alii relinquuntur numeri primi, qui sint divisores numerorum formae $2aa+bb$, nisi qui in alterutra harum formarum $8n+1$ vel $8n+3$ contineantur; quos duplicis generis numeros primos conspectui exposuisse iuvabit:

$8n+1$) 17, 41, 73, 89, 97, 113, 137, 193, 233, 241, 257, 281, 313, 337, 353, 401, 409, 433, 449, 457;

$8n+3$) 3, 11, 19, 43, 59, 67, 83, 107, 131, 139, 163, 179, 211, 227, 251, 283, 307, 331, 347, 379, 419, 443, 467, 491, 499;

atque observo hos numeros primos omnes inter numeros primos formae $2aa+bb$ ita occurrere, ut alii praeterea ibi non reperiantur.

Hinc ergo numeri huius formae $2aa+bb$, dummodo a et b sint inter se primi, praeter binarium nullos alios habent divisores primos, nisi qui sint vel huius formae $8n+1$ vel huius $8n+3$.

Cum autem omnes numeri primi in his quatuor formis $8n\pm 1$ et $8n\pm 3$ contineantur, haec observatio cum praecedente convenit.

OBSERVATIO 8

At, quod notatu maxime est dignum, observo:

Omnem numerum primum tam huius formae $8n+1$ quam huius $8n+3$ semper esse aggregatum ex quadrato et duplo quadrato; sive inter numeros primos formae $2aa+bb$ omnes plane numeros sive huius formae $8n+1$ sive huius $8n+3$ occurrere ac praeterea nullos alios.[1])

Nullus ergo assignari poterit numerus primus in harum formularum $8n+1$ et $8n+3$ alterutra contentus, qui non sit summa quadrati et dupli quadrati, et hoc quidem unico modo, si observatio prima huc trahatur.

NOTA

Proprietatum, quas hic circa numeros formae $2aa+bb$ eorumque divisores observavimus, aliae ita sunt comparatae, ut earum veritas facile ostendi possit, aliae autem maiorem demonstrationis apparatum requirunt, aliae vero

1) Theorema, quo affirmatur „omnem numerum primum, qui vel unitate vel ternario superat octonarii multiplicem, componi ex quadrato et duplo alterius quadrati", pertinet ad illas propositiones „non solum celeberrimas, sed et firmissimis demonstrationibus probatas", quas FERMATIUS in epistola a. 1658 ad KENELMUM DIGBY scripta sine demonstratione proposuit (epist. XLVI *Commercii epistolici* a WALLISIO a. 1658 primo editi), I. WALLIS, *Opera*, t. II, Oxoniae 1693, p. 857; *Oeuvres de FERMAT*, t. II, p. 402. F. R.

denique profundissimae indaginis sunt iudicandae, cum summa sollertia ad eas demonstrandas sit opus. Ad primum genus referendae sunt observationes prima, secunda, tertia, quarta et pars prior sextae; ad genus secundum autem pertinent observationes quinta, pars posterior sextae et septima, quae eo redit. Profundissimae autem indaginis est observatio octava. Proprietates autem istae similes sunt iis, quas circa summas duorum quadratorum proposui; quarum veritatem cum feliciter eruerim, operam dabo, ut etiam has proprietates observatas simili modo demonstrationibus confirmem. Incipiam ergo ab observationibus facillimis.

THEOREMA 1

1. *Si numerus N fuerit numerus formae $2aa+bb$, tum quoque eius duplum $2N$ erit numerus eiusdem formae.*

DEMONSTRATIO

Sit enim $N=2mm+nn$; erit $2N=4mm+2nn$; ponatur $2m=k$ fietque $2N=kk+2nn$ sicque $2N$ erit quoque numerus formae $2aa+bb$. Q. E. D.

COROLLARIUM 1

2. Ac si N fuerit pluribus modis numerus formae $2aa+bb$, totidem quoque modis eius duplum $2N$ erit numerus formae $2aa+bb$.

COROLLARIUM 2

3. Constat ergo veritas observationis secundae simulque ratio perspicitur, cur numerorum, qui inter numeros formae $2aa+bb$ supra expositos bis occurrunt, eorum quoque dupla ibidem bis reperiantur.

THEOREMA 2

4. *Si numerus par $2N$ fuerit numerus formae $2aa+bb$, tum quoque eius semissis N erit numerus eiusdem formae.*

DEMONSTRATIO

Posito $2N = 2mm + nn$, quo $2mm + nn$ sit numerus par, quoniam pars $2mm$ iam est par, necesse est, ut altera pars nn sit quoque numerus par ideoque et eius radix n. Ponatur ergo $n = 2k$ fietque $2N = 2mm + 4kk$, unde per 2 dividendo oritur $N = mm + 2kk$, ita ut quoque semissis N sit in forma $2aa + bb$ contentus. Q. E. D.

COROLLARIUM 1

5. Hinc etiam evidens est, si numerus propositus par $2N$ fuerit pluribus modis numerus formae $2aa + bb$, totidem quoque modis eius semissem N fore numerum eiusdem formae.

COROLLARIUM 2

6. Si ergo numerus N fuerit unico modo numerus formae $2aa + bb$, tum etiam eius duplum $2N$ unico modo erit numerus formae $2aa + bb$; si enim pluribus modis esset huius formae, totidem quoque modis eius semissis N foret eiusdem formae contra hypothesin.

COROLLARIUM 3

7. Hinc autem porro duplicando numeri $4N$, $8N$, $16N$ etc. omnes unico tantum modo in forma $2aa + bb$ continebuntur, siquidem numerus simplex N unico modo in ista forma reperiatur.

COROLLARIUM 4

8. Quod vero hic de unico modo resolutionis in formam $2aa + bb$ est dictum, patet quoque ad duos pluresve modos. Ex qualibet enim resolutione numeri N in formam $2aa + bb$ sponte nascitur resolutio numeri sive dupli sive dimidii sicque observationem tertiam demonstratam dedimus.

THEOREMA 3

9. *Si habeantur duo numeri M et N formae $2aa + bb$, erit quoque eorum productum MN numerus eiusdem formae.*

DEMONSTRATIO

Sit enim

$$M = 2aa + bb \quad \text{et} \quad N = 2cc + dd;$$

erit eorum productum

$$MN = 4aacc + 2aadd + 2ccbb + bbdd;$$

addatur $0 = 4acbd - 4acbd$ et habebitur

$$MN = 4aacc + 4acbd + bbdd + 2aadd - 4acbd + 2ccbb,$$

quae expressio manifesto est aggregatum ex quadrato et duplo quadrato, scilicet

$$MN = (2ac + bd)^2 + 2(ad - cb)^2.$$

Vel, quod eodem redit, si terminos $+4acbd$ et $-4acbd$ permutemus, ut sit

$$MN = 4aacc - 4acbd + bbdd + 2aadd + 4acbd + 2ccbb,$$

habebimus quoque alio modo

$$MN = (2ac - bd)^2 + 2(ad + cb)^2.$$

Quare si uterque numerus M et N fuerit formae $2aa + bb$, erit quoque productum numerus eiusdem formae. Q. E. D.

COROLLARIUM 1

10. Ob geminas formulas inventas productum MN erit duplici modo numerus formae $2aa + bb$. Si enim sit $M = 2aa + bb$ et $N = 2cc + dd$ ac ponatur productum $MN = 2pp + qq$, erit

$$\text{vel } p = ad - cb \quad \text{et} \quad q = 2ac + bd$$

$$\text{vel } p = ad + cb \quad \text{et} \quad q = 2ac - bd.$$

COROLLARIUM 2

11. Si fuerit vel $ad - cb$ vel $2ac - bd$ numerus negativus, pro p et q eorum valores affirmativi assumi poterunt; ex formulis enim quadratis per-

inde elicere licuisset priori casu $p = cb - ad$, posteriori vero $q = bd - 2ac$. Numeri igitur negativi hoc modo pro radicibus quadratorum oriundi calculum nihil turbant.

COROLLARIUM 3

12. Productum ergo duorum numerorum formae $2aa + bb$ duplici modo in eandem formulam resolvi poterit, nisi forte utraque resolutio ad eandem recidat, quod autem non evenit, nisi fuerit vel $cb = 0$ vel $bd = 0$ vel $ac = 0$, hoc est vel $a = 0$ vel $b = 0$ vel $c = 0$ vel etiam $d = 0$ alterque propterea numerorum propositorum vel quadratus vel duplum quadrati.

COROLLARIUM 4

13. Si ergo ambo numeri fuerint primi, eorum productum semper est duplici modo resolubile in formam $2aa + bb$, nisi alter fuerit $= 1$ vel $= 2$. Cum enim tantum excipiantur casus, quibus alter est quadratum vel duplum quadratum, uterque autem ponatur primus, excipiuntur tantum casus, quibus alter est vel 1 vel 2.

COROLLARIUM 5

14. Si ambo numeri M et N fuerint aequales seu $N = M$, ut sit $c = a$ et $d = b$, erit quidem duplici modo quadratum $MM = 2pp + qq$, scilicet vel $p = 0$ et $q = 2aa + bb$ vel $p = 2ab$ et $q = 2aa - bb$. Sed prior resolutio $MM = 2 \cdot 0^2 + (2aa + bb)^2$ minus ad scopum pertinere est censenda, quia alterum quadratum est evanescens. Sin autem esset vel $a = 0$ vel $b = 0$, utraque resolutio adeo ad unum rediret.

COROLLARIUM 6

15. Patet hinc etiam productum ex tribus numeris L, M, N formae $2aa + bb$ quadruplici modo in formam eandem resolvi posse. Sit enim

$$L = 2aa + bb, \quad M = 2cc + dd, \quad N = 2ee + ff$$

ac sit primo $LM = 2pp + qq$; erit, uti vidimus,

$$\text{vel } p = ad - cb \quad \text{et} \quad q = 2ac + bd$$

$$\text{vel } p = ad + cb \quad \text{et} \quad q = 2ac - bd.$$

Tum ergo, si ponatur productum $LMN = 2xx + yy$, erit quoque duplici modo

$$\text{vel } x = pf - eq \quad \text{et} \quad y = 2ep + fq$$
$$\text{vel } x = pf + eq \quad \text{et} \quad y = 2ep - fq.$$

Hinc ergo pro p et q valoribus inventis substituendis reperietur

$$\text{vel } x = 2ace + bde + bcf - adf \quad \text{et} \quad y = 2ade + 2acf - 2bce + bdf$$
$$\text{vel } x = 2ace - bde - bcf - adf \quad \text{et} \quad y = 2ade + 2acf + 2bce - bdf$$
$$\text{vel } x = 2ace + bde - bcf + adf \quad \text{et} \quad y = 2ade - 2acf - 2bce - bdf$$
$$\text{vel } x = 2ace - bde + bcf + adf \quad \text{et} \quad y = 2ade - 2acf + 2bce + bdf.$$

COROLLARIUM 7

16. Simili modo colligitur productum ex quatuor numeris formae $2aa + bb$ octo diversis modis in formam eandem resolvi posse; casus tamen sunt excipiendi, quibus inter numeros propositos reperiuntur vel aequales vel simplicia quadrata vel quadrata dupla; his enim casibus vidimus resolutiones, quae in genere sunt diversae, convenire.

SCHOLION

17. Quod autem ad istas resolutiones attinet, earum vis perfecte intelligi nequit, nisi demonstraverimus numeros primos plus uno modo in hac forma $2aa + bb$ non contineri. Si enim numeri primi plurimis modis essent resolubiles, de numeris compositis nihil certi definiri posset, nisi quod adhuc pluribus modis huiusmodi resolutiones admittant. Cum igitur prima observatio nos docuerit numeros primos, qui quidem in ordine numerorum formae $2aa + bb$ continentur, nonnisi semel ibidem occurrere, hanc ipsam veritatem demonstrare aggrediar.

THEOREMA 4

18. *Qui numerus duplici modo in formam $2aa + bb$ resolvi potest, is non est primus.*

DEMONSTRATIO

Sit numerus N duplici modo in hanc formam resolubilis ac ponatur

$$N = 2aa + bb \quad \text{et} \quad N = 2cc + dd,$$

ita ut tam numeri a et c quam b et d sint diversi. Multiplicetur prior aequatio per cc, altera per aa atque illa ab hac subtracta relinquet

$$(aa - cc)N = aadd - bbcc = (ad - bc)(ad + bc).$$

Quodsi iam numerus N esset primus, is in alterutro factore $ad - bc$ vel $ad + bc$ contineretur necesse est. Verum cum addendis nostris formulis sit

$$2N = 2aa + bb + 2cc + dd,$$

auferatur utrinque $2ad + 2bc$, unde habebitur

$$2N - 2ad - 2bc = 2aa + bb + 2cc + dd - 2ad - 2bc$$

sive

$$2N - 2ad - 2bc = aa + (a - d)^2 + cc + (c - b)^2.$$

At postremum hoc membrum utpote summa quatuor quadratorum certo est nihilo maius, ita ut sit

$$2N - 2ad - 2bc > 0,$$

unde fit

$$N > ad + bc.$$

Cum ergo N sit maior quam $ad + bc$ multoque magis quam $ad - bc$, numerus N in neutro factore $ad - bc$ vel $ad + bc$ tanquam pars continetur. Fieri ergo nequit, ut numerus N, qui duplici modo in formam $2aa + bb$ est resolubilis, sit primus. Q. E. D.

COROLLARIUM 1

19. Si ergo N fuerit numerus primus, certe plus uno modo in formam $2aa + bb$ non est resolubilis, quoniam, si plus uno modo resolvi posset, non esset primus, sicque habetur demonstratio observationis primae.

COROLLARIUM 2

20. Quicunque ergo numerus primus vel plane non ad formam $2aa+bb$ reduci potest vel unico tantum modo. Cavendum autem, ne hinc vicissim concludatur omnem numerum, qui unico tantum modo sit resolubilis, esse primum; huiusmodi enim conclusio regulis ratiocinandi adversaretur.

COROLLARIUM 3

21. Si fuerit idem numerus $N=2aa+bb$ itemque $N=2cc+dd$, erit hinc, ut vidimus,

$$(aa-cc)N=(ad-bc)(ad+bc)$$

ideoque

$$N=\frac{(ad-bc)(ad+bc)}{aa-cc}.$$

Numerator ergo huius fractionis non solum per denominatorem erit divisibilis, sed reductione ad integrum facta simul factores numeri N innotescent.

COROLLARIUM 4

22. Hoc ergo casu numerus N non solum non erit primus, sed etiam eius factores hinc facile colligentur. Sic cum numerus 267 bis inter numeros formae $2aa+bb$ occurrat, scilicet

$$267=2\cdot 7^2+13^2 \quad \text{et} \quad 267=2\cdot 11^2+5^2,$$

ob $a=7$, $b=13$, $c=11$ et $d=5$ habebimus

$$267=\frac{(35-143)(35+143)}{(7-11)(7+11)}=\frac{108\cdot 178}{4\cdot 18}$$

hincque

$$267=\frac{6\cdot 178}{4}=3\cdot 89.$$

THEOREMA 5

23. *Si numerus formae $2aa+bb$ fuerit divisibilis per numerum primum eiusdem formae, tum etiam quotus erit numerus eiusdem formae.*

DEMONSTRATIO

Sit numerus propositus $N = 2aa + bb$ eiusque divisor $P = 2pp + qq$; qui cum sit primus, numeri p et q erunt primi inter se. Denotet Q quotum ex hac divisione oriundum, ita ut sit

$$Q = \frac{N}{P} = \frac{2aa + bb}{2pp + qq}.$$

Cum igitur numerus $N = 2aa + bb$ sit divisibilis per $P = 2pp + qq$, erit quoque $pp(2aa + bb) = 2aapp + bbpp$ per P divisibile; at $aaP = 2aapp + aaqq$ etiam manifesto per P est divisibile, unde quoque differentiam horum numerorum $aaqq - bbpp$ per numerum primum P divisibilem esse necesse est. Quia vero est $aaqq - bbpp = (aq - bp)(aq + bp)$, alter horum duorum factorum $aq \pm bp$ per numerum primum P certo erit divisibilis. Ponatur ergo

$$aq \pm bp = mP = 2mpp + mqq$$

hincque reperitur

$$a = \frac{2mpp \mp bp}{q} + mq = \frac{p(2mp \mp b)}{q} + mq.$$

Cum itaque $\frac{p(2mp \mp b)}{q}$ sit numerus integer, numeri autem p et q inter se primi, necesse est, ut $2mp \mp b$ sit per q divisibile. Ponatur ergo $2mp \mp b = \mp nq$ eritque

$$b = nq \pm 2mp \quad \text{et} \quad a = mq \mp np.$$

Hinc autem fit

$$N = 2aa + bb$$

$$= 2mmqq \mp 4mnpq + 2nnpp + nnqq \pm 4mnpq + 4mmpp$$

sive

$$N = (2mm + nn)(2pp + qq).$$

Quodsi ergo hic numerus N dividatur per numerum primum $P = 2pp + qq$, per quem divisibilis esse ponebatur, quotus erit $Q = 2mm + nn$ ideoque numerus formae $2aa + bb$. Q. E. D.

HYPOTHESIS

24. Quoniam in sequentibus frequentissime sermo erit de numeris formae $2aa + bb$, item de numeris primis eiusdem formae, deinde vero etiam de numeris tam primis quam compositis, qui in hanc formam $2aa + bb$ non sunt

resolubiles, ne indolem horum numerorum describendo nimis fiam prolixus, compendii causa sequentibus signis utamur. Denotent ergo litterae initiales alphabeti maiusculae A, B, C, D, E etc. perpetuo in posterum numeros formae $2aa+bb$ idque in genere, sive sint primi sive compositi; eaedem vero litterae commate notatae A', B', C', D', E' etc. numeros in hac forma non contentos, sive primos sive compositos. Deinde vero litterae initiales alphabeti germanici maiusculae $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, $\mathfrak{E}$ etc. significent numeros tantum primos formae $2aa+bb$, qui sunt, ut supra vidimus, 3, 11, 17, 19, 41, 43, 59, 67, 73 etc., quibus binarius adiungi potest. Eaedem vero litterae commate notatae $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, $\mathfrak{D}'$, $\mathfrak{E}'$ etc. denotent numeros primos in forma $2aa+bb$ non contentos, qui ergo sunt 5, 7, 13, 23, 29, 31, 37, 47, 53, 61, 71 etc.

COROLLARIUM 1

25. Hac ergo notatione recepta in theoremate antecedente demonstratum est, si numerus A fuerit divisibilis per numerum $\mathfrak{A}$, quotum certo fore numerum B, vel si numerus A unum factorem habeat $\mathfrak{A}$, alterum factorem fore B, scilicet numerum formae $2aa+bb$. Vel etiam si $\frac{A}{\mathfrak{A}}$ fuerit numerus integer, erit is $=B$.

COROLLARIUM 2

26. Si ergo numerus A per numerum quempiam P divisus producat quotum B', hoc est numerum in forma $2aa+bb$ non contentum, tum divisor ille P certe non erit $\mathfrak{A}$ seu non erit numerus primus formae $2aa+bb$. Erit ergo vel compositus eiusdem formae vel plane non istius formae $2aa+bb$

COROLLARIUM 3

27. Secundum hunc autem notandi modum in theorematibus praecedentibus demonstravimus:

In primo scilicet esse $2A=B$,

in secundo vero esse $\frac{A}{2}=B$,

in tertio esse $AB=C$,

in quarto, si fuerit $A=B$ seu si idem numerus duplici modo in forma $2aa+bb$ contineatur, tum non esse $A=\mathfrak{A}$.

THEOREMA 6

28. *Si numerus formae $2aa+bb$ divisibilis fuerit per numerum, qui ista forma non contineatur, tum quotus neque erit numerus primus formae $2aa+bb$ neque productum ex meris huiusmodi numeris primis conflatum.*

DEMONSTRATIO

Demonstrari ergo debet, si numerus A divisibilis fuerit per numerum B', tum quotum neque fore $=\mathfrak{A}$ neque productum huiusmodi $\mathfrak{A}\mathfrak{B}\mathfrak{C}\mathfrak{D}$ etc. Si enim quotus esset $\mathfrak{A}$ seu $\frac{A}{B'}=\mathfrak{A}$, foret $\frac{A}{\mathfrak{A}}=B'$, quod per theorema praecedens fieri nequit. Sin autem quotus esset productum ex quotcunque numeris primis formae $2aa+bb$, scilicet $=\mathfrak{A}\mathfrak{B}\mathfrak{C}\mathfrak{D}$, ut esset $\frac{A}{B'}=\mathfrak{A}\mathfrak{B}\mathfrak{C}\mathfrak{D}$, foret utique $A=\mathfrak{A}\mathfrak{B}\mathfrak{C}\mathfrak{D}B'$ ideoque $\frac{A}{\mathfrak{A}}=\mathfrak{B}\mathfrak{C}\mathfrak{D}B'$. At est $\frac{A}{\mathfrak{A}}=B$, unde foret $B=\mathfrak{B}\mathfrak{C}\mathfrak{D}B'$ hincque $\frac{B}{\mathfrak{B}}=\mathfrak{C}\mathfrak{D}B'$; verum simili modo est $\frac{B}{\mathfrak{B}}=C$ ideoque $\frac{C}{\mathfrak{C}}=\mathfrak{D}B'$; at est $\frac{C}{\mathfrak{C}}=D$ et $\frac{D}{\mathfrak{D}}=E$; foret ergo tandem $E=B'$, quod esset absurdum. Unde sequitur quotum neque fore numerum primum formae $2aa+bb$ neque productum ex meris huiusmodi numeris primis constans. Q. E. D.

COROLLARIUM 1

29. Cum igitur quotus neque sit numerus primus formae $2aa+bb$ neque ex meris numeris primis huius formae conflatus, factores habebit vel saltem unum factorem primum in forma $2aa+bb$ non contentum seu littera $\mathfrak{A}'$ designandum.

COROLLARIUM 2

30. Quoniam ergo factores quoti sunt quoque factores dividendi, perspicuum est, si numerus formae $2aa+bb$ divisorem habeat B' seu in forma $2aa+bb$ non contentum, tum eundem numerum insuper alium ad minimum habiturum esse divisorem primum in forma $2aa+bb$ non contentum, seu si numerus A divisorem habeat B', tum certe etiam divisorem habebit alium $\mathfrak{B}'$.

COROLLARIUM 3

31. Quod hic in genere de divisoribus formae A' ostensum est, valet etiam de divisoribus formae $\mathfrak{A}'$. Hinc si numerus formae $2aa+bb$ divisibilis fuerit per numerum primum in eadem forma non contentum, tum etiam quotus est divisibilis per numerum primum in eadem forma non contentum.

THEOREMA 7

32. *Si numerus formae $2aa+bb$ quantumvis magnus divisorem habuerit numerum P neque tamen radices a et b ipsae per P sint divisibiles, tum alius numerus eiusdem formae exhiberi potest minor quam $\frac{3}{4}PP$, qui per eundem divisorem P sit divisibilis.*

DEMONSTRATIO

Posito numero $2aa+bb$ divisibili per P, quantumvis magnae fuerint radices a et b, eae semper ita exprimi possunt

$$a = mP \pm c \quad \text{et} \quad b = nP \pm d,$$

ut numeri c et d semissem ipsius P non excedant; neuterque evanescet, cum neque a neque b per P sit divisibile. Sit ergo $c < \frac{1}{2}P$ et $d < \frac{1}{2}P$; atque his valoribus substitutis forma $2aa+bb$ abibit in sequentem

$$(2mm+nn)PP \pm 4mcP \pm 2ndP + 2cc + dd;$$

quae cum sit divisibilis per P, necesse est, ut quoque eius pars $2cc+dd$ per P sit divisibilis, quae est et numerus formae $2aa+bb$ et minor quam $\frac{3}{4}PP$. Dato ergo numero formae $2aa+bb$ divisibili per numerum quemcunque P, semper exhiberi poterit numerus minor quam $\frac{3}{4}PP$ et eiusdem formae, qui per eundem numerum P futurus sit divisibilis. Q. E. D.

COROLLARIUM 1

33. Existente ergo P divisore cuiuspiam numeri A dabitur numerus $B < \frac{3}{4}PP$ per P divisibilis et quotus inde oriundus propterea erit minor quam $\frac{3}{4}P$; qui cum etiam sit divisor numeri B, si P sit divisor cuiuspiam numeri formae $2aa+bb$, hinc innotescit quoque numerus alius minor quam $\frac{3}{4}P$, qui pariter erit divisor cuiusdam numeri formae $2aa+bb$.

COROLLARIUM 2

34. Proposito porro numero quocunque P, si inter numeros formae $2aa+bb$ minores quam $\frac{3}{4}PP$ nullus datur per P divisibilis, tum etiam plane nullus existet numerus formae $2aa+bb$ per P divisibilis.

THEOREMA 8

35. *Si numerus primus in forma $2aa + bb$ non contentus fuerit divisor cuiusquam numeri huius formae neque radices seorsim per eum sint divisibiles, tum alius quoque numerus primus priore minor et in hac forma non contentus exhiberi poterit, qui etiam futurus sit divisor cuiuspiam numeri eiusdem formae, neque tamen singulae radices per eum sint divisibiles.*

DEMONSTRATIO

Demonstrandum ergo est, si fuerit numerus primus $\mathfrak{A}$ divisor cuiuspiam numeri $A = 2aa + bb$, ita ut neque a neque b per $\mathfrak{A}$ sit divisibile, tum quoque dari alium numerum primum $\mathfrak{B} < \mathfrak{A}$, qui quoque futurus sit divisor numeri cuiuspiam $B = 2cc + dd$, ita ut neque c neque d per illum sit divisibile. Demonstravimus autem exhiberi posse numerum $A < \frac{3}{4}\mathfrak{A}\mathfrak{A}$; unde si ponatur quotus $\frac{A}{\mathfrak{A}} = Q$, erit $Q < \frac{3}{4}\mathfrak{A}$ ideoque multo magis $Q < \mathfrak{A}$. At per § 31 vel hic ipse quotus Q erit numerus primus $\mathfrak{B}$ vel saltem divisorem habebit primum formae $\mathfrak{B}$. Sit igitur vel ipse quotus Q vel eius divisor $= \mathfrak{B}$, qui certe multo minor erit quam $\mathfrak{A}$. Quare cum quotus Q sit divisor numeri A, etiam $\mathfrak{B}$ erit eius divisor. Manifestum autem est hunc quotum eiusve divisorem $\mathfrak{B}$ unitatem esse non posse, cum unitas non solum sit in forma $2aa + bb$ contenta, sed etiam in demonstratione Theorematis 6 excludatur. Q. E. D.

COROLLARIUM 1

36. Si ergo numeri cuiuspiam $A = 2aa + bb$ divisor esset numerus primus $\mathfrak{A}$ in ista forma non contentus neque a et b per eum seorsim fuerit divisibile, tum alius quoque numerus primus illo minor $\mathfrak{B}$ existeret divisor numeri cuiuspiam $B = 2cc + dd$.

COROLLARIUM 2

37. Cum autem A ita capi possit, ut sit $A < \frac{3}{4}\mathfrak{A}\mathfrak{A}$, ita etiam pro altero numero $\mathfrak{B}$ inveniri poterit numerus $B < \frac{3}{4}\mathfrak{B}\mathfrak{B}$ per ea, quae in Theoremate 7 sunt demonstrata.

COROLLARIUM 3

38. Si numerus $A = 2aa + bb$ fuerit divisibilis per numerum primum $\mathfrak{A}'$ neque a et b per eum sint divisibiles, numeri a et b pro primis inter se assumi poterunt; si enim haberent communem factorem, eo sublato nihilominus praeberent numerum $2aa + bb$ per $\mathfrak{A}'$ divisibilem.

COROLLARIUM 4

39. At si numerus $A = 2aa + bb$ existentibus a et b inter se primis divisorem habeat $\mathfrak{A}'$, tum etiam numerus $B = 2cc + dd$ minor quam $\frac{3}{4}\mathfrak{A}'\mathfrak{A}'$ exhiberi poterit per $\mathfrak{A}'$ divisibilis, ita ut c et d sint inter se primi. Posito enim $a = m\mathfrak{A}' \pm c$ et $b = n\mathfrak{A}' \pm d$ (§ 32) numeri c et d certe non erunt per $\mathfrak{A}'$ divisibiles, ac si quem alium habeant communem factorem, puta $c = kp$ et $d = kq$, etiam $2pp + qq$ per $\mathfrak{A}'$ erit divisibilis existentibus p et q inter se primis hocque casu multo magis $2pp + qq$ minus erit quam $\frac{3}{4}\mathfrak{A}'\mathfrak{A}'$.

COROLLARIUM 5

40. Cum igitur existente $A = 2aa + bb$ divisibili per $\mathfrak{A}'$ et radicibus a et b inter se primis exhiberi possit numerus $B = 2cc + dd$ minor quam $\frac{3}{4}\mathfrak{A}'\mathfrak{A}'$, ita ut c et d sint numeri inter se primi, qui sit quoque per $\mathfrak{A}'$ divisibilis, erit, ut vidimus, hic idem numerus B quoque per alium numerum primum $\mathfrak{B}' < \frac{3}{4}\mathfrak{A}'$ divisibilis.

COROLLARIUM 6

41. Atque cum $B = 2cc + dd$ existentibus c et d numeris inter se primis iam sit divisibilis per numerum primum $\mathfrak{B}'$ minorem quam $\mathfrak{A}'$, inde novus numerus $C = 2ee + ff$ per $\mathfrak{B}'$ quoque divisibilis inveniri poterit, ita ut e et f sint numeri primi inter se et ipse numerus C minor quam $\frac{3}{4}\mathfrak{B}'\mathfrak{B}'$.

THEOREMA 9

42. ***Nullus datur numerus formae $2aa + bb$ existentibus a et b numeris inter se primis, qui divisibilis sit per ullum numerum primum in ista forma non contentum.***

DEMONSTRATIO

Fingamus enim per numerum primum $\mathfrak{A}$ divisibilem esse numerum $A = 2aa + bb$ atque a et b esse numeros inter se primos, hicque numerus A, si non minor fuerit quam $\frac{3}{4}\mathfrak{A}\mathfrak{A}$, in minorem transformari poterit. Habebit autem tum hic numerus A alium divisorem primum in forma $2aa + bb$ non contentum, qui sit $= \mathfrak{B}$, eritque $\mathfrak{B} < \frac{3}{4}\mathfrak{A}$; at si fuerit $A > \frac{3}{4}\mathfrak{B}\mathfrak{B}$, reperietur novus numerus $B = 2cc + dd$ divisibilis per $\mathfrak{B}$, ita ut c et d sint numeri inter se primi et $B < \frac{3}{4}\mathfrak{B}\mathfrak{B}$. Iam simili modo, cum B habeat divisorem $\mathfrak{B}$, alium praeterea habebit divisorem eiusdem indolis $\mathfrak{C} < \frac{3}{4}\mathfrak{B}$ hincque porro novus numerus $C = 2ee + ff$ per $\mathfrak{C}$ divisibilis reperietur, ut sit $C < \frac{3}{4}\mathfrak{C}\mathfrak{C}$ et e et f numeri primi inter se. Hoc modo procedendo continuo minores numeri formae $2aa + bb$ obtinerentur, qui divisibiles essent per numeros in forma $2aa + bb$ non contentos. Quare cum in minoribus numeris formae $2aa + bb$, siquidem a et b sint primi inter se, nullus occurrat, qui habeat divisorem in forma ista non contentum, ne in maximis quidem huiusmodi numeri existunt atque idcirco nullus plane datur numerus formae $2aa + bb$, qui sit divisibilis per ullum numerum in ea forma non contentum, siquidem a et b sint primi inter se. Q. E. D.

COROLLARIUM 1

43. Iam ergo evicta est veritas observationis quintae, qua animadvertimus numerum quemcunque formae $2aa + bb$, siquidem a et b sint numeri primi inter se, nullos alios habere divisores primos, nisi qui sint eiusdem formae.

COROLLARIUM 2

44. Omnis ergo numerus formae $2aa + bb$, siquidem a et b sint primi inter se, vel ipse est primus vel est productum ex duobus pluribusve numeris primis, qui omnes in forma $2aa + bb$ continentur. Huiusmodi itaque numerus nullos alios admittit divisores, nisi qui sint eiusdem formae $2aa + bb$.

COROLLARIUM 3

45. Nullus ergo numerus primus in forma $2aa + bb$ non contentus, cuiusmodi sunt 5, 7, 13, 23, 29, 31, 37, 47, 53 etc., unquam divisor vel factor

esse poterit ullius numeri formae $2aa+bb$, siquidem a et b sint numeri primi inter se. Neque vero hac restrictione, quod numeri a et b inter se primi esse debeant, est opus, dummodo uterque non sit per illum numerum primum divisibilis. Si enim a et b communem habeant divisorem n per illum numerum primum non divisibilem, ut sit $a=nc$ et $b=nd$, tum, quia $2cc+dd$ non est divisibilis, neque etiam $nn(2a+dd)$ seu $2aa+bb$ per illum erit divisibilis.

SCHOLION

46. Notetur probe vis huius demonstrationis, quae omnino est singularis et in hoc consistit, quod in minoribus numeris nullus reperiatur numerus formae $2aa+bb$ existentibus a et b numeris inter se primis, qui sit divisibilis per ullum numerum primum in ista forma $2mm+nn$ non contentum. Hinc enim conclusi etiam ne in maioribus et maximis quidem numeris nullos dari per eiusmodi numeros primos divisibiles. Demonstravi enim, si in maximis tales darentur numeri, tum etiam inter minores ac tandem minimos futuros esse numeros eiusdem indolis. Neque vero opus est ad hanc demonstrationem nosse in numeris minimis nullos dari numeros formae $2aa+bb$ per numerum primum, qui non sit eiusdem formae, divisibiles; hoc enim ipsum iam per se est absurdum minores continuo exhiberi posse numeros formae $2aa+bb$, qui per numerum primum non eiusdem formae essent divisibiles. Namque tandem necessario perveniri oporteret ad numeros primos; qui cum sint formae $2aa+bb$, certe per nullum numerum primum a se diversum dividi possent.

Quare si de quacunque alia forma $maa+bb$ existentibus a et b numeris inter se primis demonstrari posset, quodsi maiores numeri eius formae dentur per numerum primum non eiusdem formae divisibiles, tum etiam necessario minores dari numeros, qui quoque per numerum primum non eiusdem formae futuri sint divisibiles, tum tuto concludere possemus nullos plane dari numeros formae $maa+bb$, qui per ullum numerum primum in eadem forma non contentum sint divisibiles. Verum ut similis demonstratio locum habere possit, necesse est, ut $\frac{m+1}{4}$ non sit maius quam 1, alias enim Theoremata 7 et 8 applicari non possent; unde huiusmodi demonstratio non valebit nisi in formis $aa+bb$, $2aa+bb$ et $3aa+bb$. At in hac postrema quidem forma exceptionem facit divisor 2 in forma $3aa+bb$ non contentus; hoc enim casu fit $a=1$ et $b=1$ seu $3\cdot1+1$

est forma simplicissima per 2 divisibilis, quae cum non sit minor quam 2^2, quotus quoque non minor prodit quam 2 ideoque hinc conclusio ad numerum primum minorem in forma $3aa+bb$ non contentum non succedit.

THEOREMA 10

47. *Si numerus formae $2aa+bb$ unico modo in hanc formam fuerit resolubilis atque a et b fuerint primi inter se, tum ille numerus certo est primus.*

DEMONSTRATIO

Si enim non esset primus, duos pluresve haberet factores primos formae $2aa+bb$ ideoque duobus pluribusve modis in formam $2aa+bb$ esset resolubilis, ut in Theoremate 3 demonstravimus; pluralitas enim resolutionum in dubium vocari nequit, si factores illi, quos habent, fuerint inaequales. Verum etiamsi factores fuerint aequales, tamen resolutio plus uno modo succedit. Nam si numerus propositus N sit $=(2aa+bb)^2$, erit

$$\text{I. } N=2\cdot 0^2+(2aa+bb)^2$$

et

$$\text{II. } N=2(2ab)^2+(2aa-bb)^2;$$

at si sit $N=(2aa+bb)^3$, erit

$$\text{I. } N=2(2a^3+abb)^2+(2aab+b^3)^2,$$
$$\text{II. } N=2(2a^3-3abb)^2+(6aab-b^3)^2;$$

porro si sit $N=(2aa+bb)^4$, erit quoque

$$\text{I. } N=2\cdot 0^2+(4a^4+4aabb+b^4)^2,$$
$$\text{II. } N=2(4a^3b+2ab^3)^2+(4a^4-b^4)^2,$$
$$\text{III. } N=2(8a^3b-4ab^3)^2+(4a^4-12aabb+b^4)^2.$$

Ergo pluralitas resolutionum etiam locum habet, si factores fuerint aequales, dummodo resolutiones, quibus vel altera radix evanescit vel ambae communem habeant divisorem, non excludantur. Hinc ergo patet, si numerus $2aa+bb$ existentibus a et b numeris primis inter se unico modo fuerit resolubilis in hanc formam, tum eum certo esse primum. Q. E. D.

COROLLARIUM 1

48. Proposito ergo numero quocunque, quem constat esse in forma $2aa + bb$ contentum, facile erit explorare, utrum sit primus necne. Considerentur enim numeri a et b; qui si non fuerint primi inter se, statim habetur factor; sin autem sint primi, tum inde successive omnia quadrata duplicata $2aa$ subtrahentur et dispiciatur, an usquam quadratum bb relinquatur; quod si praeter casum cognitum non eveniat, certo pronunciare poterimus numerum propositum esse primum.

COROLLARIUM 2

49. Sin autem numerus propositus plus uno modo in quadratum et duplum quadratum fuerit resolubilis, tum non solum novimus eum non esse primum, sed etiam eius factores assignare poterimus secundum ea, quae § 21 sunt tradita. Hic autem modus numeros examinandi satis expedite perfici potest, perinde atque ego iam ex natura summae duorum quadratorum similem modum exposui.[1])

THEOREMA 11

50. *Nullus numerus, qui vel in hac forma* $8n - 1$ *vel in hac* $8n - 3$ *continetur, dividere potest ullum numerum formae* $2aa + bb$, *siquidem* a *et* b *sint numeri primi inter se.*

DEMONSTRATIO

Demonstrasse sufficiet nullum numerum vel formae $8n - 1$ vel $8n - 3$ unquam esse posse formae $2aa + bb$; cum enim haec forma $2aa + bb$ nullos alios admittat divisores, nisi qui in hac ipsa forma sint contenti, statim ac demonstraverimus nullum numerum vel formae $8n - 1$ vel $8n - 3$ in forma $2aa + bb$ contineri, simul certum erit ne quidem divisorem huius formae esse posse. Cum autem $8n - 1$ et $8n - 3$ sint numeri impares, videamus, quibus casibus forma $2aa + bb$ numeros impares producat; manifestum autem est hoc fieri non posse, nisi b sit numerus impar, quo casu bb fiet numerus formae $8m + 1$. Tum vero numerus a vel erit par vel impar; priori casu

1) Vide Commentationem 228 huius voluminis, imprimis § 40—52. F. R.

erit aa formae $4n$ ideoque $2aa$ formae $8n$, unde expressio $2aa + bb$ abibit in numerum formae $8m + 8n + 1$ seu $8n + 1$. Posteriori casu, quo a est numerus impar, erit aa numerus formae $4n + 1$ ideoque $2aa$ formae $8n + 2$, unde expressio $2aa + bb$ praebet hoc casu numerum formae $8m + 1 + 8n + 2$ seu formae $8n + 3$. Forma ergo $2aa + bb$ alios numeros impares non continet, nisi qui fuerint vel formae $8n + 1$ vel formae $8n + 3$. Quare nullus numerus impar vel formae $8n - 1$ vel formae $8n - 3$ unquam in forma $2aa + bb$ continetur nec propterea ullius numeri $2aa + bb$ divisor existere potest, siquidem a et b sint numeri primi inter se. Q. E. D.

COROLLARIUM 1

51. Si ergo a et b fuerint numeri primi inter se, numerus $2aa + bb$ nunquam erit divisibilis vel per 5 vel per 7 vel per ullum numerum huius seriei 5, 7, 13, 23, 29, 31, 37, 47, 53, 61, 71, 79 etc. neque etiam per ullum numerum non primum vel in forma $8n - 1$ vel in forma $8n - 3$ contentum, quales sunt 15, 21, 39, 45, 55, 63, 69, 77, 85, 87, 93, 95 etc.

COROLLARIUM 2

52. Omnes ergo numeri impares, qui unquam esse possunt divisores numerorum formae $2aa + bb$, siquidem a et b sint inter se primi, vel in hac formula $8n + 1$ vel hac $8n + 3$ continentur. Neque tamen illi numeri compositi harum formularum, qui factores habent formae $8n - 1$ vel $8n - 3$, divisores numeri $2aa + bb$ existere possunt.

COROLLARIUM 3

53. Etiamsi ergo producta $(8m - 1)(8n - 1)$, $(8m - 1)(8n - 3)$ et $(8m - 3)(8n - 3)$ in formis $8m + 1$ vel $8m + 3$ contineantur, tamen ea nunquam divisores ullius numeri formae $2aa + bb$ existere possunt, siquidem a et b fuerint numeri primi inter se.

COROLLARIUM 4

54. Quoties ergo forma $2aa + bb$ fit numerus primus, is semper vel in hac numerorum serie $8n + 1$ vel hac $8n + 3$ continebitur; unde in his duabus seriebus etiam omnes divisores primi vel saltem impares numerorum in formula $2aa + bb$ contentorum reperientur.

SCHOLION 1

55. Utrum autem omnes numeri primi, qui in seriebus numerorum $8n+1$ et $8n+3$ occurrunt, vicissim sint numeri formae $2aa+bb$, quaestio est altioris indaginis. Quousque quidem supra numeros primos formae $2aa+bb$ continuavimus, vidimus in illis omnes plane numeros primos tam huius formae $8n+1$ quam huius $8n+3$ occurrere, unde omnes quoque numeri primi in his duabus formulis contenti simul in forma $2aa+bb$ contineri videntur; verum huius veritatis demonstratio maxime est abstrusa. Viam tamen ad eam iam non parum praeparavimus, dum demonstravimus omnes divisores formae $2aa+bb$ simul esse numeros eiusdem formae, siquidem a et b fuerint inter se primi; nam proposito numero primo quocunque P sive formae $8n+1$ sive $8n+3$ si demonstrare potuerimus dari quempiam numerum $2aa+bb$ per illum divisibilem, ita ut neque a neque b per eum sit divisibile, simul erit certum numerum P esse in forma $2mm+nn$ contentum.

SCHOLION 2

56. Quod autem omnis numerus primus in alterutra harum formularum $8n+1$ et $8n+3$ contentus necessario sit aggregatum ex quadrato et duplo quadrato, uti id in numeris minoribus 500 non superantibus evenire vidimus, equidem me nondum demonstrare posse fateor [1]); haecque demonstratio multo magis ardua videtur quam ea, qua probavi omnem numerum primum formae $4n+1$ esse summam duorum quadratorum [2]). Cum autem momentum in hoc versetur, ut demonstretur proposito quocunque numero primo vel formae $8n+1$ vel formae $8n+3$ semper dari numerum $2aa+bb$ per eum divisibilem, ita ut radices a et b sint numeri inter se primi, operam is perdiderit, qui valores numerorum a et b per n expressos investigare voluerit, propterea quod hi numeri non tantum ab n pendent, sed etiam ea ratio, quod numerus $8n+1$ vel $8n+3$ sit primus, necessario in computum duci debeat. Nam si numerus $8n+1$ vel $8n+3$ non fuerit primus, evenire adeo potest, ut nullus numerus $2aa+bb$ per eum sit divisibilis. Iam equidem demonstravi per numerum $8n+1$, si sit primus, divisibiles esse omnes numeros formae $p^{8n}-q^{8n}$

1) Primam huius theorematis demonstrationem dedit I. L. LAGRANGE in celebri iam nota p. 194 laudata Commentatione, quae inscribitur *Recherches d'arithmétique.* F. R.

2) Vide Commentationes 228 et 241 huius voluminis. F. R.

et per numerum primum $8n+3$ omnes numeros formae $p^{4n+1}+q^{4n+1}$, tum vero etiam semper eiusmodi dari numeros p et q, ut priori casu forma $p^{4n}+q^{4n}$ per $8n+1$, posteriori vero forma $p^{4n+1}+q^{4n+1}$ per $8n+3$ divisibilis existat[1]). Demonstrandum igitur esset in his formis $p^{4n}+q^{4n}$ et $p^{4n+1}+q^{4n+1}$ necessario semper eiusmodi involvi casus, qui sint aggregata ex quadrato et duplo quadrato; quod autem quomodo demonstrari possit, nondum perspicio. Aeque difficile ergo ac fortasse difficilius erit sequentes propositiones[2]) demonstrare, quae tamen aeque certae videntur excepta prima, cuius demonstrationem dedi.

I. Omnis numerus primus formae $4n+1$ in hac forma $aa+bb$ continetur.

II. Omnes numeri primi in his formis $8n+1$ et $8n+3$ contenti simul in hac forma continentur $2aa+bb$.

III. Omnes numeri primi vel huius formae $12n+1$ vel huius $12n+7$ seu huius unicae $6n+1$ in hac forma $3aa+bb$ continentur.

IV. Omnes numeri primi in quapiam harum formularum $16n+1$, $16n+5$, $16n+9$, $16n+13$ vel in hac $4n+1$ contenti simul sunt numeri formae $4aa+bb$, cuius quidem demonstratio iam in prima comprehenditur.

V. Omnes numeri primi in aliqua harum formularum contenti $20n+1$, $20n+9$ simul quoque sunt formae $5aa+bb$.

VI. Omnes numeri primi in aliqua harum formularum contenti $24n+1$, $24n+7$ simul quoque sunt formae $6aa+bb$.

VII. Omnes numeri primi in aliqua harum formularum contenti $28n+1$, $28n+9$, $28n+11$, $28n+15$, $28n+23$, $28n+25$ vel, quod eodem redit, in harum aliqua $14n+1$, $14n+9$, $14n+11$ simul quoque sunt formae $7aa+bb$.

VIII. Omnes numeri primi in alterutra harum formularum contenti $24n+5$ et $24n+11$ simul sunt numeri formae $3aa+2bb$.

1) Vide huius voluminis Commentationem 134, theorema 4, et Commentationem 241. F. R.

2) Ad has propositiones vide praeter Commentationes 228 et 241 iam supra laudatas praecipue Commentationem 164 huius voluminis, imprimis notam p. 194. Vide etiam Fermatii epistolam ad Kenelmum Digby scriptam, quae nota p. 466 laudata est. F. R.

Huiusmodi autem theorematum numerus, quousque libuerit, continuari potest.

Verumtamen in iis formandis probe cavendum est, ne inductioni nimis tribuatur; neque enim, si fuerit numerus quispiam primus p in hac forma $faa + gbb$ contentus, inde generatim concludere licet omnes numeros primos formae $4fgn + p$ fore numeros eiusdem formae $faa + gbb$, etiamsi hoc, si f et g fuerint numeri exigui, verum esse videatur. Etsi enim est $67 = 5 \cdot 9 + 22 \cdot 1$ ideoque formae $5aa + 22bb$, tamen numerus $4 \cdot 5 \cdot 22n + 67$ casu $n = 2$, qui est $= 40 \cdot 22 + 67 = 947$, scilicet primus, non in forma $5aa + 22bb$ continetur; interim tamen affirmare licet, cum sit $23 = 5 \cdot 2^2 + 3 \cdot 1$ ideoque in forma $5aa + 3bb$ contineatur, omnes numeros primos $60n + 23$ in eadem forma contineri. Quodsi igitur quis methodum invenerit huiusmodi theoremata tam inveniendi quam, in quo caput rei est positum, demonstrandi, is certe in doctrina numerorum plurimum praestitisse erit iudicandus.

Admissa autem hac proprietate numerorum primorum in his formulis $8n + 1$ et $8n + 3$ contentorum plura alia hinc deduci poterunt egregia Theoremata, quorum quaedam notasse iuvabit.

THEOREMA 12

57. *Si numerus quicunque in alterutra harum formularum* $8n + 1$ *vel* $8n + 3$ *contentus nullo modo in formam* $2aa + bb$ *resolvi possit, tum non erit primus; at si unico modo in hanc formam possit resolvi, tum erit primus; sin autem plus uno modo haec resolutio succedat, tum pariter non erit primus, sed compositus.*

DEMONSTRATIO

Pars secunda et tertia ex iam demonstratis sunt manifestae. Si enim numerus propositus unico modo in forma $2aa + bb$ continetur, tum certe est primus, sin pluribus, compositus. Quod autem ad partem primam attinet, ea vi proprietatis nondum demonstratae subsistit; nam si numerus propositus esset primus, in formam $2aa + bb$ resolvi posset; quando ergo hanc resolutionem non admittit, tum certo non est primus. Q. E. D.

COROLLARIUM 1

58. Hinc igitur patet modus non difficilis propositum numerum, si fuerit vel formae $8n+3$ vel $8n+1$, explorandi, utrum sit primus necne. Subtrahantur enim ab eo successive omnia quadrata duplicata, scilicet

$$2, \quad 8, \quad 18, \quad 32, \quad 50, \quad 72, \quad 98 \quad \text{etc.},$$

quorum differentiae constituunt progressionem arithmeticam

$$6, \quad 10, \quad 14, \quad 18, \quad 22, \quad 26 \quad \text{etc.},$$

et dispiciatur, utrum uspiam quadratum relinquatur.

COROLLARIUM 2

59. Possunt etiam plures operationes simul institui ac primo successive subtrahi haec quadrata duplicata

$$2, \quad 72, \quad 242, \quad 512, \quad 882 \quad \text{etc.},$$

quorum differentiae sunt

$$70, \quad 170, \quad 270, \quad 370 \quad \text{etc.},$$

secundo vero haec quadrata duplicata

$$8, \quad 98, \quad 288, \quad 578, \quad 968 \quad \text{etc.},$$

quorum differentiae sunt

$$90, \quad 190, \quad 290, \quad 390 \quad \text{etc.},$$

tertio haec

$$18, \quad 128, \quad 338, \quad 648, \quad 1058 \quad \text{etc.},$$

quorum differentiae sunt

$$110, \quad 210, \quad 310, \quad 410 \quad \text{etc.},$$

quarto haec

$$32, \quad 162, \quad 392, \quad 722, \quad 1152 \quad \text{etc.},$$

quorum differentiae sunt

$$130, \quad 230, \quad 330, \quad 430 \quad \text{etc.},$$

quinto haec

$$50, \quad 200, \quad 450, \quad 800, \quad 1250 \quad \text{etc.},$$

quorum differentiae sunt

$$150, \quad 250, \quad 350, \quad 450 \quad \text{etc.},$$

ubi ex figuris finalibus mox patebit, quaenam operationes sint inutiles.

COROLLARIUM 3

60. A numeris autem formae $8n+1$ quadrata tantum paria duplicata subtrahi debent, unde exclusis quadratis imparibus duplicatis sequentes numeri erunt subtrahendi:

I. 8, 288, 968, 2048 etc.
280, 680, 1080
400, 400

II. 32, 392, 1152, 2312 etc.
360, 760, 1160
400, 400

III. 0, 200, 800, 1800 etc.
200, 600, 1000
400, 400

IV. 72, 512, 1352, 2592 etc.
440, 840, 1240
400, 400

V. 128, 648, 1568, 2888 etc.
520, 920, 1320
400, 400.

COROLLARIUM 4

61. Sin autem numerus sit formae $8n+3$, tum tantum quadrata imparia duplicata subtrahi debent, quae sunt:

I. 2, 242, 882, 1922 etc.
240, 640, 1040
400, 400

II. 18, 338, 1058, 2178 etc.
320, 720, 1120
400, 400

III. 50, 450, 1250, 2450 etc.
400, 800, 1200
400, 400

IV. 98, 578, 1458, 2738 etc.
480, 880, 1280
400, 400

V. 162, 722, 1682, 3042 etc.
560, 960, 1360
400, 400.

EXEMPLUM I

62. *Exploretur numerus 67579, utrum sit primus necne.*

Cum hic numerus contineatur in forma $8n + 3$, subtrahantur numerorum ordines ex Collorario 4, isque tantum secundus, tertius ac quartus, quia primus et quintus darent notam finalem 7, quae quadrato repugnat.

II.	
67579	53801
18	3520
67561	50281
320	3920
67241	46361
720	4320
66521	42041
1120	4720
65401	37321
1520	5120
63881	32201
1920	5520
61961	26681
2320	5920
59641	20761
2720	6320
56921	14441
3120	6720
53801	7721
	7120
	601

III.	
67579	53129
50	3600
67529	49529
400	4000
67129	45529
800	4400
66329	41129
1200	4800
65129	36329
1600	5200
63529	31129
2000	5600
61529	25529
2400	6000
59129	19529
2800	6400
56329	13129
3200	6800
53129	6329

IV.		
67579	52441	* 229
98	3680	
67481	48761	
480	4080	
67001	44681	
880	4480	
66121	40201	
1280	4880	
64841	35321	
1680	5280	
63161	30041	
2080	5680	
61081	24361	
2480	6080	
58601	18281	
2880	6480	
55721	11801	
3280	6880	
52441	4921	

Hic unicum occurrit quadratum $52441 = 229^2$, ut sit $67579 = 2 \cdot 87^2 + 229^2$ ideoque primus.

EXEMPLUM 2

63. *Exploretur numerus* 40081, *utrum sit primus necne.*

Cum hic numerus contineatur in forma $8n+1$, subtrahantur numeri Corollarii 3 eorumque quidem ordines II, III et IV hoc modo:

II.		III.		IV.	
40081	31889	40081	30281	40081	31369
32	2760	200	3000	72	2840
40049	29129	39881	27281	40009	28529
360	3160	600	3400	440	3240
39689	25969	39281	23881	39569	25289
760	3560	1000	3800	840	3640
38929	22409	38281	20081	38729	21649
1160	3960	1400	4200	1240	4040
37769	18449	36881	15881	37489	17609
1560	4360	1800	4600	1640	4440
36209	14089	35081	11281	35849	13169
1960	4760	2200	5000	2040	4840
34249	9329	32881	6281	33809	8329
2360	5160	2600	5400	2440	5240
31889	4169	30281	881	31369	3089

Quia igitur hic nusquam quadratum remansit, numerus propositus non est primus; est vero productum $= 149 \cdot 269$.

THEOREMA 13

64. *Si numerus n nullo modo sit aggregatum ex numero quadrato et trigonali, tum numerus $8n+1$ certe non erit primus.*

DEMONSTRATIO

Si enim n nullo modo in hac forma $aa + \frac{1}{2}(bb+b)$ continetur, tum $8n+1$ nullo modo in hac forma $8aa+4bb+4b+1$ continetur; non ergo erit numerus formae $2pp+qq$ ideoque non erit primus. Q. E. D.

COROLLARIUM

65. At si n unico modo sit aggregatum ex quadrato et trigonali, tum $8n+1$ certe erit numerus primus; sin autem sit pluribus modis, non erit primus, sed compositus.

THEOREMA 14

66. *Si numerus n nullo modo fuerit aggregatum ex numero trigonali et trigonali duplicato, tum $8n+3$ certe non erit primus.*

DEMONSTRATIO

Si enim n nullo modo in hac forma $aa+a+\frac{1}{2}(bb+b)$ continebatur, tum $8n+3$ nullo modo in hac forma $8aa+8a+2+4bb+4b+1$ ideoque nec in hac $2pp+qq$ continebitur; consequenter non erit primus. Q. E. D.

COROLLARIUM

67. At si n unico modo fuerit aggregatum ex trigonali et trigonali duplicato, tum $8n+3$ certe erit primus; sin autem fuerit plus uno modo, compositus.

THEOREMATA CIRCA RESIDUA EX DIVISIONE POTESTATUM RELICTA

Commentatio 262 indicis Enestroemiani
Novi commentarii academiae scientiarum Petropolitanae 7 (1758/9), 1761, p. 49–82
Summarium ibidem p. 8–9

SUMMARIUM

In numerorum natura plurima adhuc mysteria latere, quae non obstante summo studio, quo tam veteres quam recentiores Mathematici in proprietates numerorum inquisiverunt, adhuc nobis sunt abscondita, iam saepius est inculcatum; quod merito eo magis mirum videtur, quod prima nostra quantitatum cognitio circa numeros versari solet. Summa autem difficultas, quam in numerorum indole scrutanda offendimus, in eo potissimum consistit, quod numeri sint quantitates discretae et natura sua quasi continuitatis rationi adversentur. Non enim, ut linea parum a longitudine pedis deficiens recte dicitur fere pedalis, ita numerus parum a numero vel pari vel quadrato discrepans dici potest vel fere par vel fere quadratus; vel minima enim differentia naturam numeri vel paris vel quadrati aeque tollit, ac si esset maxima. Eodem modo etiam res se habet in divisibilitate numerorum et in residuis, quae divisione facta remanent, in quibus nulla ratio continui locum invenire potest; quare cum methodi in Analysi adhuc inventae omnes rationi continuitatis innitantur, eas frustra ad proprietates numerorum investigandas adhibemus, sed ad hoc peculiaris Analyseos species requiri videtur, cuius forsitan prima elementa etiamnum nobis sunt incognita. In lege igitur, quam residua ex divisione potestatum per divisores quoscunque relicta sequuntur, Cel. Eulerus imprimis est occupatus ac plura Theoremata affert, quorum demonstrationes summo rigore adornat; multo plures autem in hoc genere veritates agnoscere licet, quarum demonstratio frustra est quaesita, cuius rei exemplum in quantitatibus, ubi continuum spectatur, vix reperitur.

THEOREMA 1

1. *Si p sit numerus primus et a primus ad p, nullus terminus huius progressionis geometricae*

$$1, a, a^2, a^3, a^4, a^5, a^6 \text{ etc.}$$

per numerum p divisibilis existit.

DEMONSTRATIO

Patet ex EUCLIDIS Libro VII, Prop. 26[1], ubi demonstratur, si sint duo numeri a et b primi ad p, fore quoque productum ab primum ad p; ideoque, cum a sit primus ad p, erit posito $b = a$ quadratum a^2 primus ad p, hincque porro a^3 posito $b = a^2$; item a^4 posito $b = a^3$ etc. Sic igitur nulla potestas ipsius a divisibilis erit per numerum primum p.

COROLLARIUM 1

2. Si igitur singuli termini progressionis geometricae

$$1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 \text{ etc.}$$

per numerum primum p dividantur, divisio nunquam sine residuo succedet, sed ex singulis terminis orientur residua.

SCHOLION

3. Residua haec, quae ex divisione singulorum terminorum progressionis propositae geometricae per numerum primum p emergunt, hic diligentius perpendere constitui. Ac primo quidem singula haec residua, uti ex natura divisionis apparet, minora erunt numero p; nullum autem residuum erit $= 0$, quia nullus terminus per p est divisibilis. Quodsi forte prodeant residua ipso numero p maiora, ex arithmetica constat, quemadmodum ea ad minora reduci oporteat. Sic residuum $p + r$ aequivalet residuo r et in genere residuum $np + r$ redit ad residuum r; ac si r sit maius quam p, hoc residuum revocatur ad $r - p$ vel $r - 2p$ vel $r - 3p$ etc., donec ad numerum ipso p minorem perveniatur. Itaque omnia haec residua $r \pm np$ pro eodem residuo r

1) EUCLIDIS *Elementa* (ed. J. L. HEIBERG), vol. II, lib. VII prop. 24 (= 26 aliarum editionum). F. R.

reputantur. Proprie autem loquendo omnia residua sunt numeri positivi ipso divisore p minores. Verumtamen etiam saepenumero convenit et residua negativa contemplari; veluti si r sit residuum ex divisione cuiuspiam numeri per p relictum, ita ut sit $r < p$, residuum quoque erit $r - p$, numerus scilicet negativus, ita ut residuum positivum r aequivaleat residuo negativo $r - p$. Hoc modo residua ita exhiberi poterunt, ut nunquam semissem divisoris p excedant; nam si residuum affirmativum r maius fuerit quam $\frac{1}{2}p$, eius loco capiatur residuum negativum $r - p$, quod minus erit quam semissis ipsius p.

COROLLARIUM 2

4. Quoniam omnia residua sunt numeri integri iique minores quam p, sequitur plura diversa residua oriri non posse quam $p - 1$. Quare cum series geometrica $1, a, a^2, a^3, a^4, a^5$ etc. ex terminis numero infinitis constet, necesse est, ut plures termini eadem exhibeant residua.

COROLLARIUM 3

5. Sint a^μ et a^ν duo eiusmodi termini, qui idem praebeant residuum r, ita ut sit $a^\mu = mp + r$ et $a^\nu = np + r$; erit

$$a^\mu - a^\nu = (m - n)p$$

ideoque differentia horum terminorum $a^\mu - a^\nu$ per p erit divisibilis. Innumeris ergo modis differentia inter binos terminos progressionis geometricae propositae per numerum p erit divisibilis.

COROLLARIUM 4

6. Si potestas a^μ det residuum r, potestas vero a^ν residuum s fueritque $r + s = p$, quo casu dicimus residuorum r et s alterum alterius esse complementum, hoc casu summa potestatum $a^\mu + a^\nu$ per numerum p erit divisibilis. Cum enim sit $a^\mu = mp + r$ et $a^\nu = np + s$, erit

$$a^\mu + a^\nu = (m + n)p + r + s = (m + n + 1)p$$

ideoque factorem habet p.

THEOREMA 2

7. *Si potestas a^μ per p divisa praebeat residuum r et potestas a^ν residuum s, potestas $a^{\mu+\nu}$ residuum praebebit rs.*

DEMONSTRATIO

Sit enim $a^\mu = mp + r$ et $a^\nu = np + s$; erit

$$a^{\mu+\nu} = mnpp + mps + npr + rs,$$

ideoque si $a^{\mu+\nu}$ per p dividatur, residuum erit rs, quod si maius fuerit quam p, subtrahendo p, quoties fieri potest, id ad residuum ipso divisore p minus reducetur. Q. E. D.

COROLLARIUM 1

8. Cum ipsius radicis a per p divisae residuum exponi queat per a (si enim sit $a < p$, erit a residuum proprie sic dictum, sin autem $a > p$, nihilominus residuum per a exprimere licet, quia simul $a - p$ vel $a - np$ subintelligitur), si potestatis a^μ per p divisae residuum sit r, potestatis $a^{\mu+1}$ residuum erit ar, simili modo

potestatis $a^{\mu+2}$ residuum erit a^2r,
. . . $a^{\mu+3}$ . . . a^3r
etc.

COROLLARIUM 2

9. Hinc etiam sequitur, si potestatis a^μ per p divisae residuum sit $= r$, fore potestatis $a^{2\mu}$ residuum $= rr$, potestatis $a^{3\mu}$ residuum $= r^3$ etc. Ita si potestatis a^μ residuum sit $= 1$, erit omnium harum potestatum $a^{2\mu}, a^{3\mu}, a^{4\mu}, a^{5\mu}$ etc. idem quoque residuum $= 1$.

COROLLARIUM 3

10. Quodsi potestatis a^μ per p divisae residuum sit $= p - 1$, quod, ut vidimus, per -1 exponi potest, tum potestatis $a^{2\mu}$ residuum erit $= +1$,

potestatis $a^{3\mu}$ residuum $= -1$, at potestatis $a^{4\mu}$ iterum $= +1$. Atque in genere potestatis $a^{n\mu}$ residuum erit vel $+1$, si n sit numerus par, vel -1, si n sit numerus impar.

SCHOLION

11. Hinc colligitur modus satis expedite residua inveniendi, quae ex divisione cuiuscunque potestatis per numerum quemcunque relinquuntur. Veluti si residuum investigare velimus, quod ex divisione huius potestatis 7^{160} per numerum 641 oritur:

Potestates	Residua
7^1	7
7^2	49
7^3	343
7^4	478
7^8	288
7^{16}	255
7^{32}	284
7^{64}	-110
7^{128}	-79
7^{160}	-1

Nempe cum potestas prima 7 relinquat 7, potestates vero 7^2, 7^3, 7^4 relinquant 49, 343 et 478 seu -163, huius quadratum 7^8 relinquet 163^2 seu 288 et quadratum huius 7^{16} relinquet 288^2 seu 255. Simili modo potestas 7^{32} relinquet 255^2 seu 284 et potestatis 7^{64} residuum erit -110 et ex 7^{128} oritur 110^2 seu -79, quod residuum per 284 multiplicatum dabit residuum potestatis $7^{128+32} = 7^{160}$, quod erit 640 seu -1.

Novimus ergo, si potestas 7^{160} per 641 dividatur, residuum fore 640 seu -1, unde concludimus potestatis 7^{320} residuum fore $+1$. Ergo in genere potestatis 7^{160n} per 641 divisae residuum erit vel $+1$, si n sit numerus par, vel -1, si n sit numerus impar.

THEOREMA 3

12. *Si numerus a sit primus ad p formeturque haec progressio geometrica*

$$1,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6,\ a^7\ etc.,$$

innumeri in ea occurrent termini, qui per p divisi relinquunt pro residuo 1, et exponentes horum terminorum progressionem arithmeticam constituent.

DEMONSTRATIO

Quia numerus terminorum est infinitus, plura autem diversa residua oriri nequeunt quam $p-1$, necesse est, ut plures, immo infiniti termini

idem producant residuum r. Sint a^μ et a^ν duo huiusmodi termini idem residuum r relinquentes eritque $a^\mu - a^\nu$ per p divisibile. At $a^\mu - a^\nu = a^\nu(a^{\mu-\nu} - 1)$, et cum hoc productum sit divisibile per p, alter autem factor a^ν ad p sit primus, necesse est alter factor $a^{\mu-\nu} - 1$ per p est divisibile, unde potestas $a^{\mu-\nu}$ per p divisa residuum habebit $= 1$. Sit $\mu - \nu = \lambda$, ut potestatis a^λ residuum sit $= 1$, eritque omnium quoque harum potestatum $a^{2\lambda}$, $a^{3\lambda}$, $a^{4\lambda}$, $a^{5\lambda}$ etc. idem residuum $= 1$. Itaque unitas erit residuum omnium harum potestatum

$$1, \; a^\lambda, \; a^{2\lambda}, \; a^{3\lambda}, \; a^{4\lambda}, \; a^{5\lambda}, \; a^{6\lambda} \text{ etc.},$$

quarum exponentes in progressione arithmetica progrediuntur.

COROLLARIUM 1

13. Inventa ergo unica potestate a^λ, quae per p divisa residuum praebet $= 1$, infinitae inde aliae potestates exhiberi possunt, quae per p divisae quoque unitatem relinquant. Ac infima quidem huius generis potestas est $a^0 = 1$.

COROLLARIUM 2

14. Etiamsi autem praeter unitatem nulla constet potestas ipsius a, quae per p divisa unitatem pro residuo relinquat, tamen novimus infinitas huiusmodi revera dari potestates.

COROLLARIUM 3

15. Ex demonstratione porro patet dari adeo potestatem a^λ residuum $= 1$ praebentem, cuius exponens λ sit minor quam p. Si enim progressio geometrica tantum usque ad terminum a^{p-1} continuetur, quia terminorum numerus est $= p$, necesse est, ut saltem duo termini, qui sint a^μ et a^ν, idem habeant residuum; unde cum potestas $a^{\mu-\nu}$ habitura sit residuum $= 1$, ob $\mu < p$ et $\nu < p$ certe erit $\mu - \nu < p$.[1])

THEOREMA 4

16. *Si potestas a^μ per p divisa residuum relinquat $= r$ et potestatis alterius $a^{\mu+\nu}$ residuum sit $= rs$, erit potestatis a^ν, qua haec illam superat, residuum $= s$.*

1) Vide Commentationem 242 huius voluminis, § 30, imprimis notam 1. F. R.

DEMONSTRATIO

Praebeat enim potestas a^ν aliud residuum, puta $= t$, et cum potestatis a^μ residuum sit $= r$, erit potestatis $a^{\mu+\nu}$ residuum $= rt$, quod ipsi rs aequivalere deberet. Foret ergo $rt = rs + np$, siquidem ponamus residua r, t esse ipso divisore p minora. Esset ergo $t = s + \frac{np}{r}$; at cum a et p sint numeri inter se primi, omnia residua, quae ex potestatibus ipsius a per p divisis oriuntur, pariter erunt ad p prima, nisi forte sint $= 1$, ideoque, ut $\frac{np}{r}$ fiat numerus integer, necesse est, ut $\frac{n}{r}$ sit numerus integer, puta $= m$, foretque $t = s + mp$ ideoque $t = s$. Quare si potestatis a^μ residuum sit $= r$ et potestatis $a^{\mu+\nu}$ residuum $= rs$, hinc sequitur potestatis a^ν residuum fore $= s$.

COROLLARIUM 1

17. Si ergo $s = 1$ seu si duae potestates a^μ et $a^{\mu+\nu}$ idem habeant residuum r, sequitur, si maior per minorem dividatur, quoto a^ν respondere residuum $= 1$, quo ipso demonstratio praecedentis theorematis innititur.

COROLLARIUM 2

18. Si $r = 1$ et $s = 1$ seu si duae potestates a^μ et $a^{\mu+\nu}$ idem habeant residuum $= 1$, tum etiam potestas a^ν, cuius exponens est differentia illorum exponentium, pariter residuum $= 1$ habebit.

SCHOLION

19. Demonstratio huius theorematis etiam hoc modo confici potest. Cum a^μ per p divisum relinquat r, erit $a^\mu = mp + r$ similique modo $a^{\mu+\nu} = np + rs$; hinc erit $a^{\mu+\nu} - a^\mu s = np - mps = (n - ms)p$ ideoque numerus $a^{\mu+\nu} - a^\mu s = a^\mu(a^\nu - s)$ erit per p divisibilis; at alter factor a^μ per p non est divisibilis. Ergo alter $a^\nu - s$ erit per p divisibilis, consequenter potestas a^ν per p divisa residuum dabit $= s$.

THEOREMA 5

20. *Si post unitatem a^λ sit minima potestas, quae per p divisa unitatem relinquit, tum nullae aliae potestates idem residuum* $= 1$ *relinquent, nisi quae in hac progressione geometrica occurrunt*

$$1, \quad a^\lambda, \quad a^{2\lambda}, \quad a^{3\lambda}, \quad a^{4\lambda}, \quad a^{5\lambda} \quad etc.$$

DEMONSTRATIO

Ponamus enim aliam quampiam potestatem a^μ, si per p dividatur, residuum quoque dare $= 1$, et cum sit $\mu > \lambda$ neque tamen multiplo cuipiam ipsius λ aequetur, hic exponens μ ita exhiberi potest, ut sit $\mu = n\lambda + \delta$, uti sit $\delta < \lambda$; neque erit $\delta = 0$. Cum igitur tam potestas $a^{n\lambda}$ quam $a^\mu = a^{n\lambda+\delta}$ per p divisa unitatem relinquat, per § 18 haec quoque potestas a^δ unitatem pro residuo habebit foretque ergo a^δ non minima potestas huius indolis contra hypothesin. Quare si a^λ sit minima potestas residuum $= 1$ praebens, nullae aliae potestates eadem proprietate erunt praeditae, nisi quarum exponentes sunt multipla ipsius λ.

COROLLARIUM 1

21. Si ergo progressionis geometricae $1, a, a^2, a^3, a^4$ etc. iam secundus terminus a per p divisus relinquat 1, quod fit, si $a = np + 1$, tum omnes termini idem praebebunt residuum $= 1$ neque ergo in residuis ulli alii numeri praeter 1 occurrent.

COROLLARIUM 2

22. Si residuum tertii termini a^2 sit $= 1$, quod fit, si $a^2 = np + 1$, tum alterni termini $1, a^2, a^4, a^6$ etc., quorum exponentes sunt pares, omnes residuum habebunt idem $= 1$, reliqui vero termini, nisi a^1 quoque residuum habeat $= 1$, omnes alia praebebunt residua.

COROLLARIUM 3

23. Fieri ergo potest, ut in residuis multo pauciores numeri occurrant, quam numerus $p - 1$ continet unitates; plures autem quam $p - 1$ diversi numeri occurrere non possunt.

THEOREMA 6

24. *Si potestas a^{2n}, cuius exponens est numerus par, per numerum primum p divisa residuum $= 1$ relinquit, tum potestas a^n per eundem numerum p divisa dabit residuum $= +1$ vel $= -1$.*

DEMONSTRATIO

Ponamus enim r esse residuum, quod in divisione potestatis a^n per numerum primum p relinquitur, eritque potestatis a^{2n} residuum $= rr$, quod per hypothesin $= 1$. Quare erit $rr = 1 + mp$ et $rr - 1 = mp$; unde cum $rr - 1 = (r+1)(r-1)$ sit divisibile per p, alterutrum factorem $r+1$ vel $r-1$ per p divisibilem esse oportet. Priori casu erit $r + 1 = \alpha p$ et $r = \alpha p - 1$ hincque $r = -1$. Posteriori casu erit $r - 1 = \alpha p$ et $r = \alpha p + 1$ hincque $r = +1$. Ergo si potestas a^{2n} residuum praebeat $= +1$, potestas a^n habebit vel residuum $= +1$ vel $= -1$, siquidem p sit numerus primus.

COROLLARIUM 1

25. Si igitur a^{2n} fuerit minima potestas, quae per numerum primum p divisa residuum relinquit $= +1$, tum potestas a^n residuum dabit $= -1$. Ergo si minimae potestatis a^λ residuum $= 1$ praebentis exponens λ sit numerus par, tum inter residua terminorum progressionis geometricae $1, a, a^2, a^3, a^4$ etc. etiam occurret numerus -1.

COROLLARIUM 2

26. Sin autem minimae potestatis a^λ residuum 1 praebentis exponens λ sit numerus impar, tum nulla omnino potestas residuum relinquet $= -1$. Si enim quaepiam potestas, uti a^μ, daret residuum $= -1$, tum potestas $a^{2\mu}$ daret residuum $= +1$ foretque idcirco $2\mu = n\lambda$, et quia λ est numerus impar, foret $2\mu = 2m\lambda$ ideoque $\mu = m\lambda$. At potestas $a^{m\lambda}$ relinquit residuum $= +1$ neque ergo residuum -1 usquam occurrere potest.

THEOREMA 7

27. *Si a^λ fuerit minima potestas ipsius a, quae per numerum p divisa residuum praebet $= 1$, tum omnia residua, quae ex terminis progressionis geometricae*

$$1,\ a,\ a^2,\ a^3,\ \ldots\ a^{\lambda-1}$$

usque ad illam potestatem a^λ continuatae resultant, erunt inter se inaequalia.

DEMONSTRATIO

Si enim duae potestates, veluti a^μ et a^ν, quarum exponentes μ et ν sint minores quam λ, idem darent residuum, tum earum differentia $a^\mu - a^\nu$ foret per p divisibilis ideoque potestas $a^{\mu-\nu}$ per p divisa residuum relinqueret $= +1$ essetque idcirco $\mu - \nu < \lambda$ contra hypothesin; unde patet omnes potestates, quarum exponentes sint minores quam λ, diversa praebere residua.

THEOREMA 8

28. *Si a^λ fuerit quaedam potestas ipsius a, quae per numerum p divisa residuum producat $= 1$, atque progressio geometrica in membra discerpatur secundum potestates a^λ, $a^{2\lambda}$, $a^{3\lambda}$, $a^{4\lambda}$ etc. hoc modo*

$$1,\ a,\ a^2, \ldots\ a^{\lambda-1} \mid a^\lambda, \ldots\ a^{2\lambda-1} \mid a^{2\lambda}, \ldots\ a^{3\lambda-1} \mid a^{3\lambda}, \ldots\ a^{4\lambda-1}\ \text{etc.},$$

ita ut quodvis membrum λ terminos contineat, tum in quolibet membro residua prodibunt eadem atque eodem ordine recurrent.

DEMONSTRATIO

Omnium enim membrorum termini primi 1, a^λ, $a^{2\lambda}$, $a^{3\lambda}$ etc. idem praebent residuum $= 1$. Termini deinde secundi omnium membrorum a, $a^{\lambda+1}$, $a^{2\lambda+1}$, $a^{3\lambda+1}$ etc. idem pariter dabunt residuum. Sit enim r residuum ex termino a^1 ortum; quia $a^{\lambda+1} = a^\lambda a^1$, erit residuum ex hoc termino ortum $= 1 \cdot r = r$ similique modo patet terminorum $a^{2\lambda+1}$, $a^{3\lambda+1}$ etc. residua fore $= r$. Ac si in genere sit a^μ terminus quotuscunque primi membri atque residuum ex eo ortum $= r$, erit quoque termini $a^{n\lambda+\mu}$ residuum $= r$, quia termini $a^{n\lambda}$ residuum est $= 1$, hincque omnium membrorum termini analogi $a^{\lambda+\mu}$, $a^{2\lambda+\mu}$, $a^{3\lambda+\mu}$ etc. idem habebunt residuum.

COROLLARIUM 1

29. Quodsi ergo tantum terminorum in primo membro contentorum residua fuerint cognita, tum omnium quoque terminorum, qui reliqua membra constituunt, residua erunt cognita.

COROLLARIUM 2

30. Si enim proponatur terminus a^x, cuius exponens x sit numerus quantumvis magnus, eius residuum facile reperietur. Iste enim exponens x ad hanc formam $n\lambda + \mu$ reduci potest, ut sit $\mu < \lambda$, atque residuum termini a^x idem erit quod termini a^μ.

COROLLARIUM 3

31. Hic autem numerus μ minor quam λ invenitur, si numerus x per λ dividatur; tum enim residuum, quod in hac divisione remanet, erit hic ipse numerus μ, qui quaeritur.

COROLLARIUM 4

32. Semper autem datur potestas a^λ, quae per p divisa unitatem relinquit, cuius exponens λ minor sit quam numerus propositus p [§ 15], sicque ad residua omnium terminorum progressionis geometricae invenienda non opus est operationem ultra terminum a^p continuare.

COROLLARIUM 5

33. Si autem potestas a^λ sit minima earum, quae per numerum p divisae unitatem relinquunt, tunc, quia singuli termini minores quam a^λ diversa praebent residua, in residuis omnibus neque plures neque pauciores diversi numeri occurrent quam λ. Igitur si λ sit minus quam $p-1$, non omnes numeri in residuis occurrent, sed quidam numeri plane nunquam in divisione terminorum progressionis geometricae 1, a, a^2, a^3 etc. remanere poterunt.

COROLLARIUM 6

34. Si igitur diversitas residuorum spectetur, fieri potest, ut ex omnibus potestatibus ipsius a unicum tantum residuum vel duo tantum residua diversa vel tria etc. prodeant, plura tamen nunquam quam $p-1$ locum habere possunt. Quotquot autem prodierint residua, inter ea semper unitas reperitur.

THEOREMA 9

35. *Si p sit numerus primus et a primus ad p atque omnes numeri ipso p minores reperiantur inter residua, quae ex divisione omnium potestatum ipsius a per numerum primum p oriuntur, tum a^{p-1} erit minima potestas, quae per p divisa unitatem relinquit.*

DEMONSTRATIO

Sit a^λ minima potestas, quae per p divisa relinquat unitatem, atque ex praecedentibus patet esse $\lambda < p$ (§ 15). Iam cum numerus omnium residuorum diversorum sit $= \lambda$ et omnium numerorum ipso p minorum $= p-1$, patet, si esset $\lambda < p-1$, non omnes numeros minores quam p in residuis occurrere; non igitur erit $\lambda < p-1$ neque vero est $\lambda > p-1$, quia alioquin non foret $\lambda < p$. Unde relinquitur esse $\lambda = p-1$. Quocirca si omnes numeri ipso p minores in residuis occurrant, potestas a^{p-1} erit minima, quae per p divisa unitatem relinquit.

SCHOLION

36. Natura huius theorematis postulat, ut p sit numerus primus; nisi enim esset talis, fieri non posset, ut omnes numeri ipso p minores in residuis occurrerent. Quod quo clarius perspiciatur, perpendendum est, si p est numerus compositus, ad quem tamen a sit primus, nullam partem aliquotam ipsius p in residuis locum habere; nam si potestas quaepiam a^μ daret residuum r, quod esset pars aliquota ipsius p, ob $a^\mu = mp + r$ etiam ipsa potestas a^μ divisorem haberet r ideoque nec ea neque radix a esset numerus ad p primus, quod hypothesi adversatur.

THEOREMA 10

37. *Si numerus diversorum residuorum, quae ex divisione potestatum $1, a, a^2, a^3, a^4, a^5$ etc. per numerum primum p nascuntur, minor sit quam $p-1$, tum ad minimum totidem erunt numeri, qui non sunt residua, quot sunt residua.*

DEMONSTRATIO

Sit a^λ potestas minima, quae per p divisa unitatem relinquat, ac sit $\lambda < p-1$; erit numerus omnium residuorum diversorum $= \lambda$ ideoque minor

quam $p-1$. Cum ergo numerus omnium numerorum ipso p minorum sit $=p-1$, patet dari numeros in casu proposito, qui in residuis non locum obtineant. Dico autem huiusmodi numerorum ad minimum esse $=\lambda$. Quod ut ostendatur, exponamus residua per ipsos terminos, ex quibus oriuntur, eruntque haec residua

$$1, a, a^2, a^3, a^4, \ldots a^{\lambda-1},$$

quorum numerus $=\lambda$, atque haec residua, si ad formam consuetam reducantur, omnia erunt minora quam p et inter se diversa. Cum igitur sit $\lambda < p-1$ per hypothesin, dabitur certe numerus, qui in his residuis non reperitur. Sit talis numerus k; iam dico, si k non sit residuum, neque ak neque a^2k neque a^3k etc. neque $a^{\lambda-1}k$ in residuis occurrere. Fac enim $a^\mu k$ esse residuum ex potestate a^α oriundum; foret $a^\alpha = np + a^\mu k$ seu $a^\alpha - a^\mu k = np$ ideoque $a^\alpha - a^\mu k = a^\mu(a^{\alpha-\mu}-k)$ per p divisibile. At a^μ per p non est divisibile; esset ergo $a^{\alpha-\mu}-k$ per p divisibile seu potestas $a^{\alpha-\mu}$ per p divisa residuum relinqueret k, quod hypothesi repugnat. Ex quo patet omnes hos numeros

$$k, ak, a^2k, a^3k, a^4k, \ldots a^{\lambda-1}k$$

seu numeros inde derivatos non esse residua. At hi numeri, quorum multitudo $=\lambda$, omnes sunt diversi inter se; si enim duo, veluti $a^\mu k$ et $a^\nu k$, convenirent ad idemque residuum r reducerentur, foret $a^\mu k = mp + r$ et $a^\nu k = np + r$ ideoque $a^\mu k - a^\nu k = (m-n)p$ seu $(a^\mu - a^\nu)k = (m-n)p$ esset per p divisibile. Neque vero k per p est divisibile, siquidem ponimus p numerum primum et $k<p$; esset $a^\mu - a^\nu$ per p divisibilis seu $a^{\mu-\nu}$ per p divisum unitatem relinqueret, cum tamen ob $\mu < \lambda - 1$ et $\nu < \lambda - 1$ esset $\mu - \nu < \lambda$, quod esset absurdum. Ergo omnes illi numeri k, ak, a^2k, $a^3k, \ldots a^{\lambda-1}k$, si reducantur, erunt inter se diversi eorumque multitudo est $=\lambda$. Ad minimum ergo dantur λ numeri, qui in residuis locum non inveniunt, siquidem sit $\lambda < p-1$.

COROLLARIUM 1

38. Cum igitur habeantur λ diversi numeri, qui sunt residua, totidemque diversi numeri, qui non sunt residua, omnesque sint minores quam p, illorum iunctim sumtorum numerus 2λ maior esse nequit quam $p-1$, quia non plures dantur numeri ipso p minores quam $p-1$.

COROLLARIUM 2

39. Si ergo a^λ sit minima potestas, quae per numerum primum p divisa relinquit unitatem, fueritque $\lambda < p-1$, tum certum est non esse $\lambda > \frac{p-1}{2}$; erit ergo vel $\lambda = \frac{p-1}{2}$ vel $\lambda < \frac{p-1}{2}$.

COROLLARIUM 3

40. Ante [§ 15] vidimus exponentem istius potestatis minimae λ esse necessario minorem quam p. Erit ergo vel $\lambda = p-1$ vel $\lambda < p-1$; hocque casu, si $\lambda < p-1$, simul novimus iam esse vel $\lambda = \frac{p-1}{2}$ vel $\lambda < \frac{p-1}{2}$. Atque adeo intra limites $p-1$ et $\frac{p-1}{2}$ nullus continetur numerus, qui unquam esse possit valor ipsius λ.

THEOREMA 11

41. *Si p sit numerus primus atque a^λ minima potestas ipsius a, quae per p divisa unitatem relinquit, fueritque $\lambda < \frac{p-1}{2}$, tum fieri nequit, ut iste exponens λ sit maior quam $\frac{p-1}{3}$; eritque ergo vel $\lambda = \frac{p-1}{3}$ vel $\lambda < \frac{p-1}{3}$.*

DEMONSTRATIO

Cum a^λ sit minima potestas, quae per numerum primum p divisa unitatem relinquit, plures in residuis non occurrunt numeri diversi quam λ, qui relinquuntur ex his terminis

$$1,\ a,\ a^2,\ a^3,\ a^4,\ \ldots\ a^{\lambda-1},$$

si singuli per p dividantur; quare cum sit $\lambda < p-1$, habebuntur $p-1-\lambda$ numeri, qui non sunt residua; quorum si unus aliquis sit $= r$, vidimus hos omnes numeros

$$r,\ ar,\ a^2r,\ a^3r,\ a^4r,\ \ldots\ a^{\lambda-1}r,$$

siquidem dividendo per p ad numeros ipso p minores reducantur, in residuis non contineri. Hinc autem tantum λ numeri ex residuis excluduntur; quare cum sit $\lambda < \frac{p-1}{2}$, erit $\lambda < p-1-\lambda$ ideoque praeter hos numeros alii insuper dantur, qui in residuis non continentur. Sit s huiusmodi numerus, qui

neque sit residuum neque in praecedente serie non-residuorum contineatur; atque etiam hi omnes numeri

$$s,\ as,\ a^2s,\ a^3s,\ a^4s,\ \ldots\ a^{\lambda-1}s$$

non erunt residua hique numeri, uti in praecedente demonstratione ostendimus, omnes inter se erunt diversi. Neque vero ullus etiam horum numerorum, veluti $a^\mu s$, iam in praecedente serie non-residuorum continetur seu non est $a^\mu s = a^\nu r$. Nam si esset $a^\nu r = a^\mu s$, foret $s = a^{\nu-\mu} r$ vel $s = a^{\lambda+\nu-\mu} r$, siquidem esset $\mu > \nu$, unde s iam in priori serie contineretur contra hypothesin. Quocirca, si $\lambda < \frac{p-1}{2}$, dantur ad minimum adhuc λ numeri, qui non sunt residua, sicque cum λ habeamus residua et 2λ non-residua hique numeri omnes sint ipso p minores, fieri nequit, ut sit eorum summa 3λ maior quam $p-1$, seu non erit $\lambda > \frac{p-1}{3}$. Erit ergo vel $\lambda = \frac{p-1}{3}$ vel $\lambda < \frac{p-1}{3}$, siquidem sit $\lambda < \frac{p-1}{2}$ et p numerus primus.

COROLLARIUM 1

42. Si ergo non sit $\lambda < \frac{p-1}{3}$, tum certe erit $\lambda = \frac{p-1}{3}$, siquidem sit $\lambda < \frac{p-1}{2}$. At remota hac conditione si noverimus non esse $\lambda < \frac{p-1}{3}$, tum necessario sequitur esse vel $\lambda = \frac{p-1}{3}$ vel $\lambda = \frac{p-1}{2}$ vel $\lambda = p-1$.

COROLLARIUM 2

43. Sive autem sit $\lambda = \frac{p-1}{3}$ sive $\lambda = \frac{p-1}{2}$, potestas a^{p-1} per p divisa relinquit unitatem. Si enim a^λ unitatem relinquat, etiam $a^{2\lambda}$ et $a^{3\lambda}$ unitatem pro residuo dabunt.

THEOREMA 12

44. *Si a^λ sit minima potestas ipsius a, quae per numerum primum p divisa unitatem relinquit, fueritque $\lambda < \frac{p-1}{3}$, tum certe non erit $\lambda > \frac{p-1}{4}$; eritque ergo vel $\lambda = \frac{p-1}{4}$ vel $\lambda < \frac{p-1}{4}$.*

DEMONSTRATIO

Quia numerus omnium residuorum diversorum, quae ex divisione omnium potestatum ipsius a per numerum primum p proveniunt, est $= \lambda$ atque ex

his terminis nascuntur

$$1, a, a^2, a^3, a^4, \ldots a^{\lambda-1},$$

ob $\lambda < \frac{p-1}{3}$ habebuntur statim bis tot numeri, qui non sunt residua, qui ex his duabus progressionibus oriuntur

$$r, ar, a^2r, a^3r, a^4r, \ldots a^{\lambda-1}r$$

et

$$s, as, a^2s, a^3s, a^4s, \ldots a^{\lambda-1}s;$$

horum numerorum tam residuorum quam non-residuorum numerus est $= 3\lambda$ ideoque minor quam $p-1$; supererunt ergo adhuc numeri, qui non erunt residua. Sit t talis numerus atque, ut ante ostendimus, etiam hi omnes numeri

$$t, at, a^2t, a^3t, a^4t, \ldots a^{\lambda-1}t$$

non erunt residua, quorum numerus est $= \lambda$. At hi numeri non solum inter se erunt diversi, cum p sit numerus primus, sed etiam a praecedentibus discrepant sicque omnium horum numerorum sive residuorum sive non-residuorum multitudo est $= 4\lambda$, et cum singuli hi numeri sint minores quam p, impossibile est, ut sit $4\lambda > p-1$; eritque ergo vel $\lambda = \frac{p-1}{4}$ vel $\lambda < \frac{p-1}{4}$, siquidem sit, ut assumsimus, $\lambda < \frac{p-1}{3}$ et p numerus primus.

COROLLARIUM 1

45. Simili modo demonstrabitur, si sit $\lambda < \frac{p-1}{4}$, tum impossibile esse, ut sit $\lambda > \frac{p-1}{5}$, foreque idcirco vel $\lambda = \frac{p-1}{5}$ vel $\lambda < \frac{p-1}{5}$.

COROLLARIUM 2

46. In genere etiam, si constet esse $\lambda < \frac{p-1}{n}$, eodem modo demonstrabitur fieri non posse, ut esset $\lambda > \frac{p-1}{n+1}$; eritque propterea vel $\lambda = \frac{p-1}{n+1}$ vel $\lambda < \frac{p-1}{n+1}$.

COROLLARIUM 3

47. Hinc patet omnium numerorum, qui residua esse nequeant, numerum esse vel $= 0$ vel $= \lambda$ vel $= 2\lambda$ vel alii cuicunque multiplo ipsius λ; si enim plures fuerint istiusmodi numeri quam $n\lambda$, tum ob unicum statim λ novi insuper accedunt, ut eorum omnium numerus fiat $= (n+1)\lambda$; at si hic nondum omnes numeri non-residua contineantur, denuo subito λ novi accedent.

THEOREMA 13

48. *Si p sit numerus primus et a^λ minima potestas ipsius a, quae per p divisa unitatem relinquit, erit exponens λ divisor numeri $p-1$.*

DEMONSTRATIO

Numerus ergo omnium residuorum diversorum est $=\lambda$, unde numerus reliquorum numerorum ipso p minorum, qui residua esse nequeunt, erit $=p-1-\lambda$; at hic numerus (§ 47) est multiplum ipsius λ, puta $n\lambda$, ita ut sit $p-1-\lambda=n\lambda$, unde fit

$$\lambda=\frac{p-1}{n+1}.$$

Perspicuum ergo est exponentem λ esse divisorem numeri $p-1$; unde si non sit $\lambda=p-1$, certe parti cuidam aliquotae numeri $p-1$ exponens λ aequalis erit.

THEOREMA 14

49. *Si p sit numerus primus et a primus ad p, tum potestas a^{p-1} per p divisa unitatem relinquet.*

DEMONSTRATIO

Sit a^λ minima potestas ipsius a, quae per p divisa unitatem relinquit; erit, ut vidimus, $\lambda<p$ atque insuper demonstravimus esse vel $\lambda=p-1$ vel λ esse partem aliquotam numeri $p-1$. Priori casu constat propositum atque potestas a^{p-1} per p divisa unitatem relinquet. Posteriori casu, quo λ est pars aliquota numeri $p-1$, erit $p-1=n\lambda$; at cum potestas a^λ per p divisa unitatem relinquat, etiam omnes hae potestates $a^{2\lambda}$, $a^{3\lambda}$, $a^{4\lambda}$ etc. ideoque et $a^{n\lambda}$ seu a^{p-1} per p divisae unitatem relinquent. Semper ergo potestas a^{p-1} per p divisa unitatem relinquit.

COROLLARIUM 1

50. Quia potestas a^{p-1} per numerum primum p divisa unitatem relinquit, formula $a^{p-1}-1$ per numerum primum p erit divisibilis, siquidem a sit numerus ad p primus seu si a non sit divisibilis per p.

COROLLARIUM 2

51. Si ergo p sit numerus primus, omnes potestates exponentis $p-1$, veluti n^{p-1}, per p divisae vel unitatem relinquent vel nihil. Illud scilicet eveniet, si n sit numerus ad p primus, hoc vero, si ipse numerus n per p fuerit divisibilis.

COROLLARIUM 3

52. Si p sit numerus primus atque numeri a et b primi ad p, erit differentia potestatum $a^{p-1}-b^{p-1}$ per numerum p divisibilis. Cum enim tam $a^{p-1}-1$ quam $b^{p-1}-1$ per p sit divisibilis, etiam differentia harum formularum, id est $a^{p-1}-b^{p-1}$, per p erit divisibilis.

SCHOLION

53. En ergo novam demonstrationem theorematis eximii a FERMATIO quondam prolati, quae maxime discrepat ab ea, quam in Comment. Acad. Petropol. Tomo VIII dedi.[1]) Ibi enim evolutionem binomii $(a+b)^n$ in seriem modo NEWTONIANO in subsidium vocavi, quae consideratio a proposito non mediocriter abhorrere videtur; hic vero idem theorema ex solis potestatum proprietatibus demonstravi, unde haec demonstratio magis naturalis videtur, cum praeterea nobis alias insignes proprietates circa residua potestatum, quando per numeros primos dividuntur, manifestet. Patet etiam, si p sit numerus primus, non solum formulam $a^{p-1}-1$ per p esse divisibilem, sed etiam interdum fieri posse, ut etiam forma simplicior $a^{\lambda}-1$ per p sit divisibilis, tumque exponentem λ esse partem aliquotam exponentis $p-1$.

THEOREMA 15

54. *Si q sit numerus primus atque potestas a^q per numerum primum p divisa unitatem relinquat, tum a^q erit minima potestas ipsius a, quae per p divisa unitatem relinquit, nisi forte ipse numerus a per p divisus unitatem relinquit.*

---

1) Vide Commentationem 54 huius voluminis nec non notam 2, p. 34. Cf. autem etiam huius voluminis Commentationem 134, imprimis § 10. F. R.

DEMONSTRATIO

Sit enim a^{λ} minima potestas ipsius a, quae per numerum primum p divisa unitatem relinquat, atque nullae aliae potestates hac proprietate erunt praeditae nisi $a^{2\lambda}$, $a^{3\lambda}$, $a^{4\lambda}$ etc. Verum nulli harum potestas a^{q} potest esse aequalis, nisi sit $\lambda = 1$, cum q sit numerus primus, ideoque necesse est, ut sit $q = \lambda$ ideoque a^{q} minima potestas, quae per p divisa unitatem relinquit. Excipitur autem casus, quo $\lambda = 1$ seu quo ipse numerus a per p divisus unitatem relinquit; hoc enim casu omnis potestas a^{n}, sive eius exponens n sit numerus primus sive compositus, in divisione per p facienda unitatem relinquet.

COROLLARIUM 1

55. Si ergo potestas a^{q}, cuius exponens est numerus primus, per numerum primum p divisa unitatem relinquat, tum q erit pars aliquota numeri $p-1$ hocque casu formula $a^{q}-1$ per numerum primum p erit divisibilis.

COROLLARIUM 2

56. Cum q sit pars aliquota numeri $p-1$, erit $p-1=nq$ et $p=nq+1$. Quodsi ergo formula $a^{q}-1$, in qua q est numerus primus, divisibilis sit per quempiam numerum primum p, habebit hic divisor semper huiusmodi formam $p=nq+1$, nisi sit $p=a-1$; nam $a-1$ semper est divisor formulae $a^{q}-1$.

COROLLARIUM 3

57. Formula ergo $a^{q}-1$ existente q numero primo praeter divisorem $a-1$ alios divisores primos non admittit, nisi qui in hac forma $nq+1$ contineantur; et cum q sit numerus primus ideoque impar, nisi sit $q=2$, pro n nonnisi numeri pares capi possunt eruntque ergo omnes divisores, si quos habet, in forma $2nq+1$ contenti.

COROLLARIUM 4

58. Quia igitur formulae $a^{q}-1$ divisor est

$$a^{q-1}+a^{q-2}+a^{q-3}+a^{q-4}+\cdots+a^{2}+a+1,$$

haec forma in $2nq+1$ continebitur eritque ergo haec expressio

$$a^{q-1}+a^{q-2}+a^{q-3}+\cdots+a^2+a$$

per numerum primum q divisibilis, quicunque numerus sit a; at si $a=q$ vel $a=mq$, hoc est manifestum per se.

SCHOLION 1

59. Hoc etiam manifestum est, si a non sit vel q vel mq; tum enim formula inventa abit in

$$a\,(a^{q-2}+a^{q-3}+a^{q-4}+\cdots+a+1),$$

cuius factor posterior, qui transit in $\frac{a^{q-1}-1}{a-1}$, per q est divisibilis, quod quidem per se est evidens; nam cum q sit numerus primus, per eum formula $a^{q-1}-1$ est divisibilis eademque etiam per $a-1$ divisa manebit per q divisibilis, nisi $a-1$ divisorem habeat q, qui casus iam ante est exceptus. Notandum enim est formam $a^{q-1}+a^{q-2}+a^{q-3}+\cdots+a^2+a+1$ eatenus tantum in forma $2nq+1$ contineri, quatenus illa est vel numerus primus vel ex numeris primis eiusdem formae $2nq+1$ compositus. At si illa formula ipsa iam habeat factorem $a-1$, per quem forma a^q-1 est divisibilis, tum ea cum forma $2nq+1$ non conveniet. Sed si $a-1=mq$ vel $a=mq+1$, tum ipsa illa formula per q erit divisibilis, quia terminorum numerus $=q$, neque ergo illa in forma $2nq+1$ continebitur.

SCHOLION 2

60. Plurimum autem interest nosse divisores formulae a^q-1, quando q est numerus primus, quoniam ii alias excepto divisore $a-1$, qui sponte se prodit, difficillime investigantur fierique adeo potest, ut saepe huiusmodi formula, postquam est per $a-1$ divisa, fiat numerus primus. At si q non est numerus primus, sed ipse divisores habeat m, n, tum manifesto erunt hae formulae a^m-1 et a^n-1 divisores formulae a^q-1. His ergo casibus investigatio ulteriorum divisorum reducitur ad formulas a^m-1 et a^n-1, in quibus exponentes m et n sunt numeri primi. Novimus igitur, si quis tentando voluerit divisores formulae a^q-1 investigare, tentamen cum nullis aliis numeris primis, nisi qui in forma $2nq+1$ contineantur, instituendum esse, quo ipso operatio alias difficillima non mediocriter contrahitur.

THEOREMA 16

61. *Si potestas a^m per numerum p divisa residuum relinquat $= r$, tum etiam potestas $(a + \alpha p)^m$ per p divisa idem relinquet residuum r.*

DEMONSTRATIO

Si potestas $(a + \alpha p)^m$ evolvatur, prodibit

$$a^m + m\alpha a^{m-1}p + \frac{m(m-1)}{1 \cdot 2}\alpha^2 a^{m-2}p^2 + \text{etc.},$$

cuius omnes termini praeter primum per p sunt divisibiles; unde haec quantitas per p divisa idem relinquet residuum, ac si solus primus terminus a^m per p divideretur. Ergo cum potestas a^m residuum relinquat $= r$, etiam potestas $(a + \alpha p)^m$ residuum relinquet $= r$.

COROLLARIUM 1

62. Si m sit numerus par, demonstratio etiam valet pro formula $(-a + \alpha p)^m$; hoc ergo casu etiam formula $(\alpha p - a)^m$ per p divisa idem relinquit residuum r, quod formula a^m relinquit.

COROLLARIUM 2

63. At si m sit numerus impar, quia formula $-a^m$ per p divisa residuum relinquit $= -r$, etiam formula $(\alpha p - a)^m$ residuum relinquet $= -r$.

THEOREMA 17

64. *Si fuerit $a = c^n + \alpha p$, tum formula $a^{\frac{p-1}{n}}$ per numerum primum p divisa unitatem relinquet, siquidem sit n divisor numeri $p - 1$.*[1]

1) Vide etiam Commentationem 134 huius voluminis, theorema 13. F. R.

DEMONSTRATIO

Cum sit $a = c^n \pm \alpha p$, potestas $a^{\frac{p-1}{n}}$ seu $(c^n \pm \alpha p)^{\frac{p-1}{n}}$ per p divisa idem relinquit residuum ac potestas $c^{n\frac{p-1}{n}}$ seu c^{p-1}; at ob p numerum primum potestas c^{p-1} per p divisa unitatem relinquit, ergo etiam potestas $a^{\frac{p-1}{n}}$ unitatem relinquet, siquidem sit $a = c^n \pm \alpha p$ neque tamen a vel c divisibile fuerit per p.

COROLLARIUM 1

65. Ex hoc ergo theoremate cognoscuntur casus, quibus potestates numerorum, quarum exponentes sunt minores quam $p-1$, si per numerum primum p dividantur, unitatem relinquunt.

COROLLARIUM 2

66. Si ergo sit $a = cc \pm \alpha p$ existente p numero primo, tum potestas $a^{\frac{p-1}{2}}$ per p divisa unitatem relinquet seu formula $a^{\frac{p-1}{2}} - 1$ per p erit divisibilis. Cum autem p sit numerus primus, nisi sit $= 2$, semper exponens $\frac{p-1}{2}$ erit numerus integer.[1])

COROLLARIUM 3

67. Si sit $a = c^3 \pm \alpha p$, tum potestas $a^{\frac{p-1}{3}}$ per p divisa unitatem relinquet seu haec forma $a^{\frac{p-1}{3}} - 1$ per p erit divisibilis. Hic casus locum habet, si numerus primus p ita sit comparatus, ut $p-1$ per 3 sit divisibile.[2])

THEOREMA 18

68. *Si sit $ab^n = c^n \pm \alpha p$ et p numerus primus, tum potestas $a^{\frac{p-1}{n}}$ per p divisa unitatem relinquet, siquidem $\frac{p-1}{n}$ fuerit numerus integer.*[3])

1) Vide etiam Commentationem 134 huius voluminis, theorema 11, nec non huius voluminis Commentationem 242, § 30. F. R.

2) Vide etiam Commentationem 134 huius voluminis, theorema 12. F. R.

3) Vide etiam Commentationem 134 huius voluminis, theorema 14. F. R.

DEMONSTRATIO

Potestas $(c^n \pm \alpha p)^{\frac{p-1}{n}}$ seu $a^{\frac{p-1}{n}} b^{p-1}$ per p divisa idem relinquit residuum quod potestas $c^{n \cdot \frac{p-1}{n}} = c^{p-1}$; at haec potestas unitatem relinquit, ergo et potestas $a^{\frac{p-1}{n}} b^{p-1}$. Huius autem factor b^{p-1} pariter unitatem relinquit; ergo necesse est alterum quoque factorem $a^{\frac{p-1}{n}}$, si per p dividatur, unitatem relinquere, nisi sit b vel c divisibile per p.

COROLLARIUM 1

69. Si ergo sit $ab^n = c^n \pm \alpha p$, seu $ab^n - c^n$ sive $c^n - ab^n$ per numerum primum p divisibile, tum haec quoque formula $a^{\frac{p-1}{n}} - 1$ per p erit divisibilis.

COROLLARIUM 2

70. Cum p sit numerus primus, ponatur $p = mn + 1$, atque si fuerit haec formula $ab^n - c^n$ seu $c^n - ab^n$ per p divisibilis, tum etiam haec formula $a^m - 1$ per numerum primum p erit divisibilis.

COROLLARIUM 3

71. Dummodo ergo pro b et c eiusmodi numeri dentur, ut $ab^n - c^n$ seu $c^n - ab^n$ divisionem per numerum primum $p = mn + 1$ admittat, tum certum est hanc formulam $a^m - 1$ per eundem numerum primum $p = mn + 1$ esse divisibilem.

THEOREMA 19

72. *Si formula $a^m - 1$ fuerit divisibilis per numerum primum $p = mn + 1$, tum semper dantur numeri x et y eiusmodi, ut $ax^n - y^n$ sit per eundem numerum primum p divisibilis.*

DEMONSTRATIO

Cum enim x^{mn} et y^{mn} per p divisae unitatem relinquant, formula $a^m x^{mn} - y^{mn}$ semper erit per p divisibilis, dummodo neque x neque y per p

sit divisibile. Cum iam per factores sit

$$a^m x^{mn} - y^{mn} = (ax^n - y^n)(a^{m-1}x^{mn-n} + a^{m-2}x^{mn-2n}y^n + a^{m-3}x^{mn-3n}y^{2n} + \dots + y^{mn-n}),$$

si quis neget factorem primum $ax^n - y^n$ unquam esse per p divisibilem, is affirmare cogitur alterum factorem semper esse per p divisibilem, dummodo pro x et y non capiantur numeri per p divisibiles. Retineat x valorem quemcunque, at pro y ponamus successive numeros 1, 2, 3, 4 usque ad $p-1=mn$, ne unquam obtineat valorem per p divisibilem, sitque brevitatis gratia

$$A = a^{m-1}x^{mn-n} + a^{m-2}x^{mn-2n} \quad + \dots + 1,$$
$$B = a^{m-1}x^{mn-n} + a^{m-2}x^{mn-2n}2^n \quad + \dots + 2^{mn-n},$$
$$C = a^{m-1}x^{mn-n} + a^{m-2}x^{mn-2n}3^n \quad + \dots + 3^{mn-n},$$
$$\vdots$$
$$N = a^{m-1}x^{mn-n} + a^{m-2}x^{mn-2n}(mn)^n + \dots + (mn)^{mn-n}$$

ac forent omnes hae quantitates $A, B, C, \dots N$, quae progressionem algebraicam ordinis $mn-n$ constituunt, per p divisibiles hincque etiam earum differentiae primae, secundae, tertiae et ordinis cuiusvis. At huius seriei differentia ordinis $mn-n$, quae tantum per terminos $mn-n+1$ seriei definitur neque adeo terminum $(mn+1)^{mn-n}$ seu p^{mn-n} involvit, quia p non potest esse valor ipsius y, est, uti constat,

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots (mn-n),$$

quae aperte non est per numerum primum $p = mn+1$ divisibilis, quia nullos alios habet divisores primos, nisi qui sint minores quam $mn-n$. Cum igitur haec differentia ordinis $mn-n$ non sit divisibilis per p, sequitur non omnes terminos seriei $A, B, C, D, \dots N$ esse per p divisibiles. Illo igitur casu vel illis casibus ipsius y, quibus termini huius seriei non sunt per p divisibiles, necessario alter factor $ax^n - y^n$ per p erit divisibilis.

COROLLARIUM 1

78. Quicunque ergo numerus pro x sumatur modo per p non divisibilis, pro y semper datur valor $< p$, qui reddit formulam $ax^n - y^n$ per p divisibilem. Similique modo, si pro y numerus pro lubitu assumatur, demonstrari potest semper pro x eiusmodi numerum $< p$ inveniri posse, quo eadem formula per p divisibilis evadat.

COROLLARIUM 2

74. Si ergo $a^m - 1$ fuerit divisibile per numerum primum $mn + 1 = p$ atque pro x capiatur numerus quicunque b per p non divisibilis, semper inveniri potest numerus y, ut haec forma $ab^n - y^n$ seu $y^n - ab^n$ fiat per $p = mn + 1$ divisibilis.

COROLLARIUM 3

75. Simili modo si forma $a^m - 1$ fuerit divisibilis per numerum primum $p = mn + 1$ atque pro y capiatur numerus quicunque c per p non divisibilis, semper inveniri poterit numerus x, ut haec forma $ax^n - c^n$ seu $c^n - ax^n$ fiat per $p = mn + 1$ divisibilis.

THEOREMA 20

76. *Si haec forma $ab^n - c^n$ vel $c^n - ab^n$ fuerit divisibilis per numerum primum $p = mn + 1$, tum sumto numero d pro lubitu, dummodo per p non sit divisibilis, semper inveniri potest numerus x, ut vel haec forma $ax^n - d^n$ vel haec $ad^n - x^n$ vel $d^n - ax^n$ vel $x^n - ad^n$ fiat per eundem numerum primum $p = mn + 1$ divisibilis.*

DEMONSTRATIO

Cum haec forma $ab^n - c^n$ vel $c^n - ab^n$ sit per numerum primum $p = mn + 1$ divisibilis, tum etiam hic numerus $a^m - 1$ per eundem numerum primum $p = mn + 1$ erit divisibilis (§ 71). Verum si $a^m - 1$ per p est divisibilis, sumto numero quocunque d per p non divisibili dabitur numerus x, ut vel haec forma $ax^n - d^n$ vel etiam haec $ad^n - x^n$ vel $d^n - ax^n$ vel $x^n - ad^n$ fiat quoque per numerum primum $p = mn + 1$ divisibilis.

COROLLARIUM

77. Posito ergo $d = 1$ si formulae $ab^n - c^n$ divisor sit numerus primus $p = mn + 1$, tum dabitur numerus x, ut vel haec forma $ax^n - 1$ vel $a - x^n$ vel $x^n - a$ fiat per eundem numerum primum p divisibilis.

SCHOLION

78. Theorema undevicesimum, quod inversum est theorematis duodevicesimi, iam alibi[1]) proposueram, sed sine demonstratione, et tametsi tum eius demonstrationem multis modis tentavi, eam tamen invenire non potui, donec in methodum hic usitatam incidi, quae igitur eo magis notatu digna videtur, cum dubium sit nullum, quin eadem ad multa alia numerorum arcana viam sit patefactura. Haec quoque methodus, quae in consideratione differentiarum continetur, nuper mihi insigni usui fuit, dum eius beneficio tandem pulcherrimi theorematis FERMATIANI, quo omnis numerus primus formae $4n+1$ aggregatum duorum quadratorum esse affirmatur, demonstrationem sum consecutus[2]), ad quam ante nullo alio modo pervenire potui.

1) Vide huius voluminis Commentationem 134, § 63. F. R.

2) Vide huius voluminis Commentationem 241, sed etiam Commentationem 228. F. R.

SOLUTIO PROBLEMATIS DE INVESTIGATIONE TRIUM NUMERORUM QUORUM TAM SUMMA QUAM PRODUCTUM NEC NON SUMMA PRODUCTORUM EX BINIS SINT NUMERI QUADRATI[1]

Commentatio 270 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 8 (1760/1), 1763, p. 64—73
Summarium ibidem p. 12—14

SUMMARIUM

Etsi huius generis problemata plerisque Geometris nimis sterilia videntur, quam ut in iis solvendis operam suam collocare aequum iudicent, negari tamen nequit, quin inde insignia incrementa Analysis acceperit. Ac certe in genere affirmare licet, quo magis cuiusquam problematis resolutio fuerit abscondita methodisque adhuc cognitis frustra tentata, eo magis solutionis, si tandem successerit, pretium esse constituendum. Ad hoc autem genus omnino referendum videtur problema hic pertractatum, cuius difficultatem non solum plures conatus irriti, antequam ad solutionem pervenire licet, suscipiendi, sed etiam magnitudo numerorum satisfacientium manifesto declarat. Quam quidem solutionem Cel. Auctor tanquam simplicissimam affert, ea maximis numeris continetur; verum hic non parum intererit observasse ex ipsa Auctoris solutione multo minores numeros quaestioni satisfacientes satis expedite elici posse. Positis enim ternis quaesitis numeris nx, ny, nz, ut tres sequentes numeros

$$\text{I.}\quad n(x+y+z),\qquad \text{II.}\quad nn(xy+xz+yz),\qquad \text{III.}\quad n^3xyz$$

1) Vide etiam Commentationem 427 (indicis ENESTROEMIANI): *Problematis cuiusdam DIOPHANTEI evolutio*, Novi comment. acad. sc. Petrop. 17 (1772), 1773, p. 24; *LEONHARDI EULERI Opera omnia*, series I, vol. 3. F. R.

quadratos effici oporteat, prima et tertia conditio impletur sumendo

$$z = \frac{vv(x+y)}{xy-vv} \quad \text{et} \quad n = m^2xy(x+y)(xy-vv).$$

Ut autem secunda impleatur, statuit Auctor

$$xy - vv = uu, \quad x = tv,$$

ut sit

$$y = \frac{vv+uu}{tv} \quad \text{et} \quad z = \frac{vv}{uu}(x+y);$$

tum vero deducitur ad hanc aequationem

$$\frac{vv}{uu} = \frac{tt+1-ss}{2s(tt+1)-3tt-2},$$

cui facillime[1]) satisfit sumendo $s = \frac{3}{2}$, siquidem hinc sequitur $\frac{vv}{uu} = tt - \frac{5}{4}$. Capi ergo convenit $t = \frac{pp+5qq}{4pq}$, unde fit $\frac{v}{u} = \frac{5qq-pp}{4pq}$, ubi numeros p et q pro lubitu assumere licet, ita ut hinc innumerabiles solutiones obtineantur; inter quas simplicissima videtur, quae oritur sumendo $t = \frac{3}{2}$, unde fit $v = 1$ et $u = 1$, porro $x = \frac{3}{2}$, $y = \frac{4}{3}$ et $z = \frac{17}{6}$. Iam ob $x + y + z = \frac{17}{3}$ capiatur $n = 6 \cdot 34$ ex prima conditione sicque tres numeri satisfacientes minimi erunt

$$\text{I. } 9 \cdot 34 = 306, \quad \text{II. } 8 \cdot 34 = 272, \quad \text{III. } 17 \cdot 34 = 578,$$

quorum summa est

$$= 1156 = 34^2,$$

summa productorum ex binis

$$= 89 \cdot 34^2 + 9 \cdot 17 \cdot 34^2 + 8 \cdot 17 \cdot 34^2 = 19^2 \cdot 34^2,$$

productum omnium

$$= 8 \cdot 9 \cdot 17 \cdot 34^3 = 8^2 \cdot 3^2 \cdot 17^4.$$

---

1) Abhinc Summarium discrepat ab iis, quae in ipsa dissertatione exponuntur, ubi imprimis non inveniuntur sequentes solutiones simplicissimae, scilicet numeri 306, 272, 578. Quae discrepantia explicatur eo, quod EULERUS Summarium dissertationis ante a. 1756 (cf. notam p. 530) conscriptae nonnisi a. 1762 Academiae Petropolitanae tradidit. Extant enim haec verba in epistola d. 21. Sept. 1762 ad. G. F. MÜLLER scripta: „Hiermit habe ich die Ehre Ew. Hochedelgeb. meine Auszüge aus dem VIII Tom. Nov. Comment. zu überschicken, wovon einige als besondere Abhandlungen angesehen, und in den Conferenzen vorgelesen werden könnten, wann Dieselben solches für nöthig erachteten." Vide G. ENESTROEM, *Verzeichnis der Schriften* LEONHARD EULERS, Leipzig 1910/3, p. 214; LEONHARDI EULERI *Opera omnia*, series III. F. R.

Hinc pronunciari posse videtur minimos numeros integros problemati satisfacientes esse

$$272, \ 306, \ 578,$$

fractos autem hos

$$\frac{1}{2}, \ \frac{4}{17}, \ \frac{9}{34}.$$

Ceterum hic notasse iuvabit, si tres numeri integri x, y, z desiderentur, ut tantum haec formula $xy + xz + yz$ fiat numerus quadratus, eos in genere ita exhiberi posse, ut sit

$$x + y = (a - b)^2 + (d - e)^2,$$
$$y + z = (b - c)^2 + (e - f)^2,$$
$$z + x = (c - a)^2 + (f - d)^2,$$

unde fit

$$x + y + z = aa + bb + cc - ab - bc - ac + dd + ee + ff - de - ef - df$$

ipsique numeri ita se habebunt

$$x = (a - b)(a - c) + (d - e)(d - f),$$
$$y = (b - c)(b - a) + (e - f)(e - d),$$
$$z = (c - a)(c - b) + (f - d)(f - e),$$

unde fit

$$\sqrt{(xy + yz + xz)} = a(e - f) + b(f - d) + c(d - e).$$

Vel simplicius haec solutio ita enunciari potest, ut sit

$$x = lm + pq, \quad y = mn + qr, \quad z = nl + rp$$

sumtis his senis numeris l, m, n et p, q, r ita, ut sit

$$l + m + n = 0 \quad \text{et} \quad p + q + r = 0;$$

tum vero erit

$$\sqrt{(xy + yz + xz)} = lq - mp = mr - nq = np - lr.$$

1. Etsi problemata huius generis, quae DIOPHANTEA appellari solent, parum utilitatis affere videntur, tamen certum est Analysin mathematicam atque adeo etiam eam partem, quae circa infinita versatur, ex methodo problemata DIOPHANTEA solvendi maxima incrementa cepisse. Non solum autem huiusmodi problemata, si sint difficiliora, fines Analyseos plurimum amplificaverunt, sed etiam vim ingenii mirifice acuere solent, ut etiam in aliis problematibus, quomodo solutionem institui oporteat, facilius perspicere valeat. Quamobrem

huius generis problemata, praecipue si modus solvendi magis fuerit reconditus, minime contemnenda esse arbitror. Dum enim singularia artificia ad eorum solutionem requiruntur, ab iisdem quoque egregia subsidia ad universam Analysin uberius excolendam expectare licebit.

2. Ad hoc autem genus potissimum referendum videtur problema propositum, quandoquidem id diu et multum per varia methodi DIOPHANTEAE artificia frustra tractavi, ut fere etiam de eius solutione penitus desperaverim. Tandem vero, quasi inopinato, solutionem sum consecutus, quae eo magis notatu digna videbatur, quod minimi numeri, quos quidem adhuc satisfacientes elicere potui, sunt ita praegrandes, ut mirum non sit solutionem tantis difficultatibus fuisse involutam. Quare cum methodo singulari ad istam solutionem pertigerim, eius ampliorem explicationem usu non esse carituram arbitror, cum simili fortasse modo aliae quaestiones multo adhuc difficiliores superari queant.

3. Quaeruntur ergo tres numeri, quibus tres sequentes conditiones conveniant:

I. Ut eorum summa sit numerus quadratus,

II. ut summa productorum ex binis sit numerus quadratus,

III. ut productum omnium trium sit numerus quadratus.

Quod problema etiam hoc modo enunciari potest, ut quaeratur aequatio cubica $z^3 - pzz + qz - r = 0$ omnes suas radices habens rationales, cuius singuli coefficientes p, q et r sint numeri quadrati. Posset adhuc adiici haec conditio, ut isti numeri sint integri; verum per se est perspicuum, quomodo inventis ternis numeris fractis satisfacientibus ex iis facile integri, qui etiam satisfaciant, formari queant. Quicunque enim terni numeri satisfacere fuerint inventi, iidem per numerum quadratum quemcunque multiplicati aeque satisfacient, quo pacto fractiones facillime tollentur.

4. Sint igitur nx, ny, nz tres huiusmodi numeri quaesiti ac satisfieri oportebit his conditionibus:

I. Ut sit $n(x + y + z) =$ quadrato,

II. ut sit $nn(xy + xz + yz)$ seu $xy + xz + yz =$ quadrato,

III. ut sit n^3xyz seu $nxyz =$ quadrato.

At primae et tertiae conditioni satisfiet, si reddatur

$$xyz(x+y+z) = \text{quadrato.}$$

Ponatur ergo

$$xyz(x+y+z) = vv(x+y+z)^2,$$

unde per $x+y+z$ dividendo erit $xyz = vv(x+y+z)$ hincque

$$z = \frac{vv(x+y)}{xy-vv}.$$

Cum igitur hinc fiat $xyz = \frac{vvxy(x+y)}{xy-vv}$, ut $nxyz$ prodeat quadratum, capi debet

$$n = m^2xy(x+y)(xy-vv).$$

Hisque valoribus pro z et n assumtis satisfactum erit primae et tertiae conditioni.

5. Hinc itaque nostri tres numeri erunt:

Primus $nx = mmxxy(x+y)(xy-vv)$,
secundus $ny = mmxyy(x+y)(xy-vv)$,
tertius $nz = mmvvxy(x+y)^2$,

ubi per numerum arbitrarium m fractiones, si quae forte occurrent, tolli poterunt.

Verum contemplemur iam secundam conditionem, quae ob $z = \frac{vv(x+y)}{xy-vv}$ requirit, ut sit

$$xy + \frac{vv(x+y)^2}{xy-vv} = \text{quadrato.}$$

Ponamus in hunc finem

$$xy - vv = uu,$$

ut sit

$$y = \frac{vv+uu}{x} \quad \text{et} \quad z = \frac{vv(x+y)}{uu};$$

erit

$$xy = vv+uu \quad \text{et} \quad x+y = \frac{xx+vv+uu}{x}$$

efficiendumque est, ut sit

$$vv+uu+\frac{vv(xx+vv+uu)^2}{uuxx} = \text{quadrato.}$$

6. Ponatur $x = tv$, ut sit $y = \frac{vv + uu}{tv}$, esseque debet

$$vv + uu + \frac{(vv(tt+1) + uu)^2}{ttuu} = \text{quadrato}$$

seu multiplicando per $ttuu$

$$ttuuvv + ttu^4 + v^4(tt+1)^2 + 2uuvv(tt+1) + u^4 = \text{quadrato}$$

sive

$$v^4(tt+1)^2 + uuvv(3tt+2) + u^4(tt+1) = \text{quadrato}.$$

Statuatur huius quadrati radix $= vv(tt+1) + suu$; erit

$$vv(3tt+2) + uu(tt+1) = 2svv(tt+1) + ssuu,$$

unde elicitur

$$\frac{vv}{uu} = \frac{tt+1-ss}{2s(tt+1) - 3tt - 2} = \text{quadrato}.$$

Sit porro $s = t - r$ et habebitur

$$\frac{vv}{uu} = \frac{2rt - rr + 1}{2t^3 - (2r+3)tt + 2t - 2(r+1)}.$$

Multiplicetur numerator et denominator per $2rt - rr + 1$, ut fiat

$$\frac{vv}{uu} = \frac{(2rt - rr + 1)^2}{4rt^4 - 2(3rr + 3r - 1)t^3 + (2r^3 + 3rr + 2r - 3)tt - 2(3r-1)(r+1)t + 2(r-1)(r+1)^2}.$$

7. Tota ergo quaestio huc est perducta, ut huius fractionis denominator reddatur quadratum; posito enim

$$4rt^4 - 2(3rr + 3r - 1)t^3 + (2r^3 + 3rr + 2r - 3)tt$$
$$- 2(3r-1)(r+1)t + 2(r-1)(r+1)^2 = QQ$$

erit definitis hinc t et r

$$\frac{v}{u} = \frac{2rt - rr + 1}{Q},$$

tum vero

$$x = tv \quad \text{et} \quad y = \frac{vv + uu}{tv},$$

unde numeri quaesiti definientur. Ante autem, quam ad istam aequationem

pertigimus, solutionem iam limitavimus positione $xy - vv = uu$, quae restrictio probe est notanda, quoniam nullum est dubium, quin eiusmodi extent solutiones, in quibus $xy - vv$ non sit numerus quadratus, easque propterea hinc non reperiemus. Verum hanc limitationem ideo facere sum coactus, ut ad istam formulam quadrato aequandam pervenire licuerit, quippe quae ita est comparata, ut per cognita artificia resolvi possit. Sicque tota solutionis vis in reductionibus paragraphi praecedentis est sita.

8. Pluribus autem casibus haec formula et quidem infinitis modis quadratum effici potest, quorum praecipui, et qui statim se offerunt, sunt: I. Si coefficiens ipsius t^4, scilicet $4r$, seu r fuerit numerus quadratus; II. si terminus ultimus $2(r-1)(r+1)^2$ seu $2(r-1)$ fuerit numerus quadratus. Utroque enim casu per regulas cognitas valores idonei pro t elici, tum vero porro ex quolibet alii novi inveniri possunt. Sin autem simul et r et $2(r-1)$ fuerint quadrata, una operatione plures valores idoneos pro t eruere licet, neque vero hic, ut plerumque fieri solet, solutio simplicior se offert; etsi enim, si $2(r-1) =$ quadrato, satisfacit valor $t = 0$, tamen inde prodit $x = 0$ et $y = \infty$, qui valores pro natura quaestionis plane sunt incongrui. Excluduntur enim solutiones, quibus unus trium numerorum quaesitorum evanesceret, quia tum quaestio esset facillima et circa duos numeros versaretur, quorum tam summa quam productum esset quadratum.

CASUS 1 QUO PONITUR $r = 1$

9. Hic casus simplicissimus videtur, quia ultimus terminus nostrae formae evanescit primusque fit quadratus. Habemus ergo

$$4t^4 - 10t^3 + 4tt - 8t = QQ \quad \text{et} \quad \frac{v}{u} = \frac{2t}{Q}.$$

Ad hanc aequationem solvendam statuamus

$$Q = 2tt - \frac{5}{2}t$$

eritque

$$4tt - 8t = \frac{25}{4}tt, \quad \frac{9}{4}t = -8 \quad \text{et} \quad t = -\frac{32}{9}.$$

At hinc fiet

$$\frac{v}{u} = \frac{4}{4t-5} = \frac{-36}{173},$$

unde habebimus $v = -36$, $u = 173$, $t = \frac{-32}{9}$ et

$$x = tv = 128 \quad \text{indeque porro} \quad y = \frac{36^2 + 173^2}{128} = \frac{31225}{128} = \frac{25 \cdot 1249}{128}.$$

Erit ergo

$$x + y = \frac{47609}{128} \quad \text{et} \quad z = \frac{36^2 \cdot 47609}{173^2 \cdot 128}$$

ac tres numeri quaesiti erunt ob $xy - vv = uu$:

$$\text{Primus} = \frac{128^2 \cdot 25 \cdot 1249 \cdot 47609 \cdot 173^2}{128 \cdot 128} mm,$$

$$\text{secundus} = \frac{128 \cdot 25^2 \cdot 1249^2 \cdot 47609 \cdot 173^2}{128^2 \cdot 128} mm,$$

$$\text{tertius} = \frac{36^2 \cdot 128 \cdot 25 \cdot 1249 \cdot 47609^2}{128 \cdot 128^2} mm.$$

10. Ad fractiones tollendas ponamus $m = \frac{128}{5}$ eruntque terni nostri numeri:

$$\left.\begin{aligned} \text{Primus} &= 128^2 \cdot 173^2 \cdot 1249 \cdot 47609 = 128^2 \cdot 173^2 \\ \text{secundus} &= 5^2 \cdot 173^2 \cdot 1249^2 \cdot 47609 = 5^2 \cdot 173^2 \cdot 1249 \\ \text{tertius} &= 36^2 \cdot 1249 \cdot 47609^2 \quad = 36^2 \cdot 47609 \end{aligned}\right\} \text{in } 1249 \cdot 47609,$$

quibus numeris evolutis erit

$$\begin{aligned} \text{primus} &= 490356736 \cdot 59463641, \\ \text{secundus} &= 934533025 \cdot 59463641, \\ \text{tertius} &= 61701264 \cdot 59463641, \end{aligned}$$

quorum productum manifesto est quadratum, quippe

$$5^2 \cdot 36^2 \cdot 128^2 \cdot 173^4 \cdot 1249^4 \cdot 47609^4.$$

Summa autem reperitur

$$25 \cdot 59463641^2$$

et summa productorum ex binis

$$173^2 \cdot 59463641^2 \cdot 18248924559376,$$

cuius radix quadrata est

$$173 \cdot 59463641 \cdot 4271876.$$

11. Pro eadem aequatione resolvenda poni potest

$$Q = 2tt - \frac{5}{2}t - \frac{9}{16},$$

ut tres primores termini tollantur, ac prodibit

$$-8t = +\frac{45}{16}t + \frac{81}{256} \quad \text{seu} \quad 0 = 173t + \frac{81}{16}, \quad \text{ergo} \quad t = \frac{-81}{16 \cdot 173}.$$

Hinc

$$Q = \frac{81^2}{128 \cdot 173^2} + \frac{405}{32 \cdot 173} - \frac{9}{16} = -\frac{9 \cdot 207563}{128 \cdot 173^2} \quad \text{et} \quad \frac{v}{u} = \pm\frac{144 \cdot 173}{207563}.$$

Sumi enim potest valor ipsius Q tam negative quam positive. Statuatur ergo $v = -144 \cdot 173$, $u = 207563$; erit

$$x = 9 \cdot 81 = 729 \quad \text{et} \quad y = \frac{vv + uu}{729},$$

unde iam manifestum est ad tam enormes perveniri numeros, ut solutio praecedens prae hac multo simplicior sit aestimanda. Superfluum autem foret huiusmodi solutiones nimis complicatas ulterius evolvere, quia in huius generis quaestionibus solutione simplicissima plerumque contenti esse solemus.

CASUS 2 QUO PONITUR $r = \frac{3}{2}$

12. Hac positione ultimus formulae nostrae terminus fit quadratum eritque $\frac{v}{u} = \frac{12t - 5}{4Q}$ existente

$$QQ = 6t^4 - \frac{41}{2}t^3 + \frac{27}{2}tt - \frac{35}{2}t + \frac{25}{4}.$$

Iam ad tres terminos ultimos tollendos statuatur

$$Q = \frac{5}{2} - \frac{7}{2}t + \frac{1}{4}tt$$

eritque

$$6t^4 - \frac{41}{2}t^3 = \frac{1}{16}t^4 - \frac{7}{4}t^3 \quad \text{et} \quad t = \frac{60}{19}$$

hincque

$$Q = \frac{4375}{732} \quad \text{et} \quad \frac{v}{u} = \frac{19}{14},$$

unde $v = 19$ et $u = 14$. Nunc igitur erit

$$x = tv = 60 \quad \text{et} \quad y = \frac{vv + uu}{x} = \frac{557}{60} \quad \text{ideoque} \quad x + y = \frac{4157}{60}$$

et tres numeri quaesiti

$$\text{primus} \quad = \frac{60^2 \cdot 557 \cdot 4157 \cdot 196}{60 \cdot 60} mm = 14^2 \cdot 60^2 \cdot 557 \cdot 4157,$$

$$\text{secundus} = \frac{60 \cdot 557^2 \cdot 4157 \cdot 196}{60 \cdot 60 \cdot 60} mm = 14^2 \cdot 557^2 \cdot 4157,$$

$$\text{tertius} \quad = \frac{361 \cdot 60 \cdot 557 \cdot 4157^2}{60 \cdot 60 \cdot 60} mm = 19^2 \cdot 557 \cdot 4157^2$$

posito $m = 60$; hique numeri iam notabiliter sunt minores quam ii, qui casu primo sunt inventi.

13. Quoniam ergo hi numeri ob parvitatem attentione digni videntur, ii ita exhibeantur:

$$\begin{aligned} \text{Primus} &= 705600 \cdot 2315449, \\ \text{secundus} &= 109172 \cdot 2315449, \\ \text{tertius} &= 1500677 \cdot 2315449. \end{aligned}$$

Quorum numerorum summa est

$$= 2315449^2$$

et productum

$$= 14^4 \cdot 19^2 \cdot 60^2 \cdot 557^4 \cdot 4157^4$$

sicque uterque numerus quadratus. At summa productorum ex binis erit

$$(14^2 \cdot 60^2 \cdot 14^2 \cdot 557 + 14^2 \cdot 60^2 \cdot 19^2 \cdot 4157 + 14^2 \cdot 557 \cdot 19^2 \cdot 4157) 2315449^2,$$

quae reducitur ad hanc formam

$$14^2 \cdot 2315449^2 \cdot 6631333489,$$

cuius radix quadrata est

$$14 \cdot 2315449 \cdot 81433.$$

Sunt autem hi numeri circiter 15000 vicibus minores quam primum inventi.

CASUS 3 QUO PONITUR $r = 3$

14. Posito $r = 3$ fit $\frac{v}{u} = \frac{6t-8}{Q}$ et habebitur haec aequatio resolvenda

$$QQ = 12t^4 - 70t^3 + 84tt - 64t + 64.$$

Iam ad ternos ultimos terminos tollendos statuatur

$$Q = 8 - 4t + \frac{17}{4}tt$$

eritque

$$12t^4 - 70t^3 = \frac{289}{16}t^4 - 34t^3,$$

unde elicitur

$$t = -\frac{576}{97} \quad \text{et} \quad Q = \pm\frac{8 \cdot 213601}{97 \cdot 97}.$$

Ergo

$$\frac{v}{u} = -\frac{97 \cdot 529}{213601} = -\frac{97 \cdot 23}{9287} = -\frac{23 \cdot 97}{37 \cdot 251}$$

ideoque $v = -23 \cdot 97$ et $u = 37 \cdot 251$, tum

$$x = tv = 23 \cdot 24^2 \quad \text{et} \quad y = \frac{91225730}{23 \cdot 24^2}.$$

Verum facile perspicitur hos numeros in immensum excrescere, unde iis evolvendis supersedemus. Contemplemur ergo adhuc unum casum, quo tam primus quam ultimus terminus formulae QQ fiunt quadrati.

CASUS 4 QUO PONITUR $r = 9$

15. Posito $r = 9$ fit $\frac{v}{u} = \frac{18t - 80}{Q}$ existente

$$QQ = 36t^4 - 538t^3 + 1716tt - 520t + 1600.$$

Tollamus terminos primum et duos ultimos ponendo

$$Q = 40 - \frac{13}{2}t \pm 6tt$$

et habebimus

$$-538t^3 + 1716tt = \mp 78t^3 \pm 480tt + \frac{169}{4}tt,$$

unde elicimus pro utroque signo,

$$\text{superiori } t = \frac{5 \cdot 191}{16 \cdot 23},$$

$$\text{inferiori } t = \frac{5 \cdot 1723}{32 \cdot 77};$$

utrinque autem prodeunt numeri nimis magni.

Tollamus ergo tres terminos ultimos ponendo

$$Q = 40 - \frac{13}{2}t + \frac{1339}{64}tt;$$

hinc autem numeri multo adhuc maiores resultant. Posset porro pro binis terminis primis cum ultimo tollendis poni $Q = 6tt - \frac{260}{6}t + 40$, verum hinc multo minus ad numeros simpliciores perveniemus.

16. Ex his satis tuto concludi posse videtur minimos numeros problemati satisfacientes[1]) esse eos, quos § 13 elicuimus, qui ergo, si penitus per multiplicationem evolvantur, erunt:

$$\begin{aligned} \text{Primus} &= 1633780814400, \\ \text{secundus} &= 252782198228, \\ \text{tertius} &= 3474741058973. \end{aligned}$$

Sin autem in fractionibus numeri satisfacientes simplicissimi desiderentur, ii indidem assignari poterunt his per 2315449^2 dividendis, ita ut hi numeri futuri sint:

$$\text{Primus} = \frac{705600}{2315449},$$

$$\text{secundus} = \frac{196}{4157},$$

$$\text{tertius} = \frac{361}{557},$$

quorum tam summa quam summa productorum ex binis et omnium trium productum sunt numeri quadrati.

1) Vide epistolam ab EULERO ad CHR. GOLDBACH d. 23. Aug. 1755 datam, *Correspondance math. et phys. publiée par P. H. Fuss*, St.-Pétersbourg 1843, t. I, p. 627; LEONHARDI EULERI *Opera omnia*, series III. At vide imprimis simplicissimas illas solutiones

272, 306, 578,

quae in Summario huius dissertationis p. 520—521 expositae sunt. F. R.

THEOREMATA ARITHMETICA NOVA METHODO DEMONSTRATA[1])

Commentatio 271 indicis Enestroemiani
Novi commentarii academiae scientiarum Petropolitanae 8 (1760/1), 1763, p. 74—104
Summarium ibidem p. 15—18

SUMMARIUM

Singulari omnino Auctor hic utitur methodo ad plures insignes numerorum proprietates demonstrandas, quarum quidem nonnullas iam alio modo demonstratas dedit; reliquae vero novae sunt habendae atque ad alias maiori adhuc attentione dignas viam parare videntur. Ipsa quidem methodus ita dilucide est exposita, ut nihil ad ampliorem eius illustrationem afferri possit; at vero praecipuas veritates, quas Auctor feliciter investigavit, hic recensuisse iuvabit.

Postquam is iam gemina[2]) methodo eximium illud Theorema, *quod forma* $a^{p-1}-1$ *semper sit divisibilis per numerum* p, *siquidem is sit primus neque numerus* a *per eum dividi possit,* demonstrasset, hic non solum tertiam demonstrationem ex aliis principiis petitam adiicit, verum etiam idem Theorema, quod ad numeros tantum primos erat adstrictum, ad omnes plane numeros extendit. Proposito scilicet quocunque numero N definit inde numerum n, ut forma a^n-1 per illum numerum N certe divisionem admittat; ubi quidem numerus a pro lubitu assumi potest, sed tamen ita comparatus esse debet, ut cum numero N nullum habeat divisorem communem seu ut numeri N et a sint inter se primi, quae quidem conditio semper est subintelligenda, etiamsi verbis non exprimatur. Demonstrat igitur Auctor exponentem n semper ita pendere a numero proposito N, ut aequalis sit multitudini numerorum ipso N minorum, qui simul ad eum sint primi, id quod exemplo

1) Vide etiam Commentationem 564 (indicis Enestroemiani): *Speculationes circa quasdam insignes proprietates numerorum*, Acta acad. sc. Petrop. 1780: II (1784), p. 18; *Leonhardi Euleri Opera omnia*, series I, vol. 4. F. R.

2) Vide notam p. 534. F. R.

magis perspicuum reddetur. Sit igitur numerus propositus $N = 10$; numeri autem eo minores ad eumque primi sunt 1, 3, 7, 9 ideoque quatuor, unde fit $n = 4$. Sumto iam pro a numero quocunque ad 10 primo, seu qui neque per 2 neque per 5 dividatur, ac certo pronunciare licet hanc formam $a^4 - 1$ esse per 10 divisibilem, hoc est, omnium huiusmodi numerorum biquadrata unitate minuta divisionem per 10 admittunt. Veluti si $a = 3$, fit $a^4 - 1 = 80$; si $a = 7$, fit $a^4 - 1 = 2400$, et ita porro.

Quaeritur autem hic ante omnia, quomodo pro quovis numero N multitudo numerorum ipso minorum ad eumque primorum, cui numerus n aequalis est sumendus, commode definiri possit; ubi quidem perspicuum est, si N fuerit numerus primus, fore $n = N - 1$, propterea quod omnes numeri ipso minores, quorum multitudo utique est $= N - 1$, simul ad eum sunt primi. Sed si numerus N non est primus, eius ratio compositionis ex primis est spectanda; ubi cum existentibus p, q, r, s etc. numeris primis omnes numeri ad hanc formam $p^\alpha q^\beta r^\gamma s^\delta$ etc. revocari possint, ab Auctore est demonstratum:

Si sit $N = p^\alpha$, fore

$$n = p^{\alpha-1}(p-1) = N \cdot \frac{p-1}{p};$$

si $N = p^\alpha q^\beta$, fore

$$n = p^{\alpha-1}(p-1) \cdot q^{\beta-1}(q-1) = N \cdot \frac{p-1}{p} \cdot \frac{q-1}{q};$$

si $N = p^\alpha q^\beta r^\gamma$, fore

$$n = p^{\alpha-1}(p-1) \cdot q^{\beta-1}(q-1) \cdot r^{\gamma-1}(r-1) \quad \text{seu} \quad n = N \cdot \frac{p-1}{p} \cdot \frac{q-1}{q} \cdot \frac{r-1}{r};$$

sicque porro, ita ut pro dato numero N numerus n inveniri possit ex solis numeris primis in eum ingredientibus nullo ad eorum potestates habito respectu, quod in dissertatione non est animadversum.[1]) Ita si $N = 120$, qui numerus ex primis 2, 3, 5 componitur, inde fit $n = 120 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 32$; atque forma $a^{32} - 1$ certe erit divisibilis per 120, dum a nullum horum numerorum 2, 3, 5 complectatur.

Verum hic insuper observare licet plerumque minorem potestatem eadem proprietate praeditam esse. Rationem enim harum demonstrationum perpendenti mox patebit, si fuerit $N = p^\alpha q^\beta r^\gamma$, formam $a^n - 1$ per hunc numerum fore divisibilem, non solum cum n fuerit productum ex his tribus numeris $p^{\alpha-1}(p-1)$, $q^{\beta-1}(q-1)$, $r^{\gamma-1}(r-1)$, sed sufficere, si pro n minimus communis dividuus horum numerorum accipiatur, quae observatio haud inelegans in dissertatione est praetermissa.[1]) Ita si sit $N = 120 = 2^3 \cdot 3 \cdot 5$, terni numeri pro exponente n inveniendo sunt 4, 2, 4, quorum minimus communis dividuus est 4, sicque pronunciare licet hanc formam $a^4 - 1$ semper esse per 120 divisibilem, dummodo a ad 120 fuerit primus. Simili modo si $N = 63 = 3^2 \cdot 7$, hi duo factores dant numeros 6 et 6; quo-

1) De huius dissertationis Summario similia valent iis, quae nota p. 520 de Summario Commentationis 270 exposita sunt. F. R.

rum minimus communis dividuus cum sit 6, haec forma $a^6 - 1$ erit per 63 divisibilis, si modo a neque ternarium neque septenarium contineat. Sit $N = 32760 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$, qui factores inter se primi praebent hos numeros 4, 6, 4, 6, 12, quorum communis dividuus est 12; ex quo haec forma $a^{12} - 1$ semper per 32760 divisionem admittit, modo a nullum horum numerorum primorum 2, 3, 5, 7, 13 involvat; veluti si $a = 11$, est

$$a^{12} - 1 = 3138428376720 = 32760 \cdot 95800622,$$

ubi notari convenit esse $95800622 = 2 \cdot 37 \cdot 61 \cdot 19 \cdot 1117$. Saepenumero autem evenire potest, ut pro sumto numero a etiam minor potestas satisfaciat, sed talis diminutio ab indole numeri a pendet neque in genere minor potestas, quam hic est assignata, theoremati tribui potest.

Praeter varias computandi operationes, quae vulgo in Arithmetica tradi solent huiusque disciplinae quasi partem practicam constituunt, eiusdem pars theoretica, quae in indaganda numerorum natura versatur, non minus iam olim tractari est coepta, quemadmodum ex EUCLIDE et DIOPHANTO intelligere licet, ubi insignes numerorum proprietates erutae reperiuntur ac demonstratae. Quo magis autem deinceps numerorum indolem et affectiones Mathematici sunt scrutati, multo plures eorum proprietates observaverunt, unde pulcherrima Theoremata numerorum naturam illustrantia derivavere, quae partim demonstrationibus sunt munita, partim etiamnunc iis indigent, sive quod eae ab auctoribus non sint inventae sive temporum iniuria deperditae; ex quo genere plurima passim occurrunt huiusmodi Theoremata numerica, quorum demonstrationes adhuc desiderantur, etiamsi eorum veritatem in dubium vocare non liceat. Atque hic insigne discrimen, quod inter Theoremata arithmetica et geometrica intercedit, non parum mirari debemus, quod vix ulla propositio geometrica proferri possit, quam non sit in promtu sive veram sive falsam ostendere, dum contra multae circa numerorum naturam notae sunt propositiones, quarum veritatem nobis agnoscere, neutiquam vero demonstrare liceat.

Magna huiusmodi Theorematum copia a FERMATIO relicta habetur, quorum demonstrationes maximam partem se invenisse affirmavit, quas cum eius scriptis interiisse in eximium huius scientiae detrimentum non parum est dolendum. Quot autem talium Theorematum demonstrationes vel sunt cognitae vel restitutae, in iis certe multo maior vis ingenii elucet, quam

vix in ullo alio demonstrationum genere deprehendimus; unde in hoc negotio non tam utilitas, qua scientia numerorum illustratur, est aestimanda, quam maxima subtilitas, qua huiusmodi demonstrationes prae aliis distinguuntur. Atque ob hanc causam, cum iam saepius, quam plerisque aequum videri queat, in hoc genere laboraverim, operam mihi equidem non perdidisse videor neque etiamnunc Theoremata, quae hic propono, utilitate caritura confido.

Notatu imprimis dignum visum est Theorema illud Fermatii, quo omnes numeros in hac formula $a^{p-1}-1$ contentos semper divisibiles esse per numerum p, siquidem is fuerit primus neque tamen a per eum divisionem admittat, affirmavit, cuius Theorematis iam geminam[1]) dedi demonstrationem. Nunc autem idem in latiori sensu contemplor atque in genere, si divisor non sit numerus primus, sed quicunque N, investigo, cuiusmodi exponentem potestati cuicunque tribui oporteat, ut expressio a^n-1 semper sit divisibilis per numerum N, dummodo numerus a cum eo nullum habeat divisorem communem. Inveni autem hoc semper usu venire, quoties exponens n aequalis fuerit multitudini numerorum ipso N minorum, qui sint ad N primi. Ad hoc ergo demonstrandum ante omnia huiusmodi theorematibus est opus, ex quibus proposito numero quocunque N cognosci possit, quot inter numeros ipso minores futuri sint ad eum primi, seu qui nullum cum eo habeant communem divisorem; quae theoremata iam ipsa multo ampliorem usum habere atque ad alias magis absconditas numerorum proprietates aditum parare videntur. Iis autem praemissis demonstratio veritatis propositae ita est comparata, ut maiore attentione non indigna videatur.

THEOREMA 1

1. *Si per numerum quemcunque n termini progressionis arithmeticae cuiuscunque, cuius differentia sit numerus ad n primus, dividantur, inter residua occurrent omnes numeri divisore n minores.*

DEMONSTRATIO

Sit progressionis arithmeticae terminus primus $=a$ et differentia $=d$, quae sit ad n numerus primus seu quae cum numero n nullum praeter uni-

1) Revera Eulerus adeo tres huius theorematis Fermatiani demonstrationes dederat, quarum duae quidem priores ex eodem fonte fluunt. Quae demonstrationes inveniuntur in Commentationibus 54, 134, 262 huius voluminis. F. R.

tatem habeat divisorem communem, ita ut progressio arithmetica futura sit

$$a, \quad a+d, \quad a+2d, \quad a+3d, \quad a+4d, \quad a+5d \quad \text{etc.},$$

ac dico, si singuli termini per numerum n dividantur, inter residua omnes numeros ipso n minores occurrere. Ad hoc demonstrandum sufficiet huius progressionis tantum n terminos considerasse, qui sunt

$$a, \quad a+d, \quad a+2d, \quad a+3d, \ldots a+(n-1)d.$$

Quodsi ergo isti termini singuli per n dividantur, omnia residua inter se diversa esse oportet. Si enim duo termini, veluti $a+\mu d$ et $a+\nu d$ existentibus μ et ν numeris ipso n minoribus, per n divisi paria praeberent residua, eorum differentia $(\nu-\mu)d$ utique per n esset divisibilis. Cum autem numeri d et n nullum habeant divisorem communem, necesse esset, ut $\nu-\mu$ divisionem per n admitteret; id quod esset absurdum ob $\nu-\mu<n$. Quare cum omnia illa residua sint diversa eorumque numerus utpote terminorum numero aequalis sit $=n$, in iis omnes plane numeri ipso n minores occurrent, scilicet

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad 5, \ldots n-1,$$

siquidem differentia progressionis d sit numerus ad divisorem propositum n primus. Q. E. D.

COROLLARIUM 1

2. Inter terminos ergo progressionis arithmeticae cuiuscunque, quorum numerus est n, dummodo differentia eius ad n sit numerus primus, certe reperitur unus, qui per n est divisibilis; tum vero etiam aderit unus, qui per n divisus datum residuum r relinquit.

COROLLARIUM 2

3. Si ergo numerus d ad n fuerit primus, semper numerus huius formae $a+\nu d$ exhiberi potest existente a numero quocunque et ν minore quam n, qui per numerum n sit divisibilis, atque etiam sub iisdem conditionibus semper talis dabitur numerus $a+\nu d$, qui per n divisus datum relinquat residuum r.

COROLLARIUM 3

4. Datis igitur numeris a et d, quorum hic d ad n sit primus, semper invenire licet numeros μ et ν, ut aequationi huic

$$a + \nu d = \mu n$$

vel etiam huic

$$a + \nu d = \mu n + r$$

satisfiat, quicunque numerus minor quam n pro r assumatur.

SCHOLION

5. Quod de progressionis arithmeticae terminorum numero n demonstravimus, id de tota progressione in infinitum continuata valet; termini enim, qui post illos n terminos sequuntur, eadem ordine reproducunt residua, si per n dividantur. Ita terminorum post $a + (n-1)d$ sequentium, qui sunt $a + nd$, $a + (n+1)d$, $a + (n+2)d$ etc., per n divisorum residua conveniunt cum residuis ex terminis initialibus a, $a + d$, $a + 2d$ etc. natis. Atque si tota series in infinitas periodos distribuatur cuique n terminos tribuendo hoc modo

$$a,\ a+d, \ldots a+(n-1)d \,|\, a+nd, \ldots a+(2n-1)d \,|\, a+2nd, \ldots a+(3n-1)d \,| \ldots,$$

termini cuiuslibet periodi eadem praebebunt residua eodemque ordine disposita; omnium enim periodorum termini cum primi tum secundi et tertii etc. constanter paria dabunt residua. Quare si rationem residuorum cognoscere velimus, sufficit unicam periodum examinasse.

THEOREMA 2

6. *In progressione arithmetica, cuius terminorum numerus est* $= n$, *totidem termini erunt ad numerum* n *primi, quot inter numeros ipso* n *minores dantur ad* n *primi, dummodo differentia progressionis fuerit ad* n *numerus primus.*

DEMONSTRATIO

Sit enim a terminus primus et d differentia progressionis, quae sit ad n numerus primus, ideoque ipsa progressio n continens terminos

$$a, \quad a + d, \quad a + 2d, \quad a + 3d, \ \ldots \ a + (n-1)d.$$

Quoniam igitur, si hi termini per numerum n dividantur, inter residua occurrunt omnes plane numeri ipso n minores, ponamus ex termino quocunque

$a + \nu d$ resultare residuum r ac manifestum est, si r fuerit numerus ad n primus, illum quoque terminum $a + \nu d$ ad n fore primum, sin autem r cum n habeat quempiam divisorem communem, idem quoque erit divisor communis numerorum n et $a + \nu d$. Quare quot inter numeros ipso n minores fuerint numeri ad n primi, totidem quoque inter terminos progressionis arithmeticae propositae habebuntur numeri ad n primi. Q. E. D.

COROLLARIUM 1

7. Si n fuerit numerus primus, quia omnes numeri ipso minores ad ipsum quoque sunt primi, quorum numerus ergo est aequalis $n - 1$, in illa etiam progressione arithmetica omnes termini praeter unum erunt ad n primi, quippe unus per n est divisibilis.

COROLLARIUM 2

8. Sin autem n fuerit numerus compositus, inter numeros ipso minores dabuntur quipiam, qui cum eo divisorem habeant communem, totidemque vero etiam reperientur in progressione arithmetica, quibus iidem communes divisores cum n conveniant.

COROLLARIUM 3

9. Ita si sit $n = 6$, quia inter numeros senario minores sunt duo ad 6 primi, scilicet 1 et 5, in omni progressione arithmetica sex terminorum

$$a, \quad a + d, \quad a + 2d, \quad a + 3d, \quad a + 4d, \quad a + 5d$$

duo tantum erunt ad 6 primi, dummodo differentia d sit ad 6 numerus primus. Ita si capiatur $a = 4$, $d = 5$, horum sex numerorum 4, 9, 14, 19, 24, 29 duo, scilicet 19 et 29, ad 6 sunt primi, unus 24 per 6 divisibilis, reliqui vero 4, 9, 14 ad 6 compositi perinde ac 2, 3, 4.

SCHOLION

10. Haec Theoremata in doctrina et contemplatione naturae numerorum insignem habent usum, hic autem ea solum adhibere visum est ad hanc quaestionem enodandam, *proposito numero quocunque n, quot inter numeros ipso*

minores futuri sint ad eundem numerum n primi. Statim quidem patet, si n sit numerus primus, omnes numeros ipso minores simul ad eum fore primos eorumque idcirco numerum esse $= n - 1$. Verum si n sit numerus compositus, multitudo numerorum ipso minorum ad eumque primorum est minor; quanta autem sit quovis casu, non tam facile assignari potest. Ita si sit $n = 12$, inter numeros minores tantum quatuor reperiuntur ad 12 primi, scilicet

$$1, \ 5, \ 7, \ 11;$$

et si sit $n = 60$, numeri minores ad eum primi sunt

$$1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59,$$

quorum numerus est 16, unde reliqui 43 omnes cum 60 divisores habent communes. Moneri hic convenit unitatem ad omnes plane numeros esse numerum primum, etiamsi omnium sit divisor; id quod ex definitione est evidens, qua numeri dicuntur esse inter se primi, qui praeter unitatem alium nullum agnoscunt divisorem.

THEOREMA 3

11. *Si n sit potestas quaecunque numeri primi p seu $n = p^m$, inter numeros ipso minores tot erunt ad eum primi, quot unitates continentur in*

$$p^m - p^{m-1} = p^{m-1}(p-1).$$

DEMONSTRATIO

Multitudo omnium numerorum potestate $n = p^m$ minorum est $p^m - 1$; inter hos autem reperiuntur quidam, qui ad n non sunt primi, omnia scilicet ipsius p multipla minora quam n nullique alii praeterea; ex quo sequentes numeri ad n non erunt primi

$$p, \quad 2p, \quad 3p, \quad 4p, \quad \ldots \, p^m - p,$$

quorum numerus est $p^{m-1} - 1$; quo ablato a numero omnium ipso $n = p^m$ minorum relinquitur multitudo eorum, qui ad p^m sunt primi, quorum numerus itaque est $= p^m - p^{m-1} = p^{m-1}(p-1)$. Q. E. D.

COROLLARIUM 1

12. Hinc igitur primo sequitur, id quod per se est manifestum, si sit $n = p$ existente p numero primo, numerum omnium numerorum ipso minorum ad eumque primorum esse $= p - 1$, siquidem omnes numeri ipso minores simul sunt ad eum primi.

COROLLARIUM 2

13. At si sit $n = p^2$, inter numeros ipso minores multitudo eorum, qui ad eum sunt primi, est $= pp - p = p(p-1)$; reliqui, quorum numerus est $p - 1$, ad $n = p^2$ erunt compositi seu per p divisibiles.

COROLLARIUM 3

14. Proposita autem numeri primi potestate quacunque $n = p^m$ inter numeros ipso minores, quorum multitudo est $= p^m - 1$, reperiuntur $p^{m-1} - 1$, qui sunt per p divisibiles ideoque ad p^m non primi; reliqui vero omnes, quorum numerus est $= p^m - p^{m-1} = p^{m-1}(p-1)$, ad p^m sunt primi.

SCHOLION

15. Si ergo numerus propositus n fuerit potestas cuiuspiam numeri primi, ope huius regulae assignare poterimus, quot inter omnes numeros ipso minores futuri sint ad eum primi. Quando autem numerus n ex duobus pluribusve numeris primis fuerit conflatus, hinc nondum ista quaestio confici potest; praecedentibus autem Theorematibus adhibendis istam quaestionem latius patentem resolvere poterimus.

THEOREMA 4

16. *Si numerus n sit productum duorum numerorum primorum p et q seu $n = pq$, multitudo omnium numerorum ipso minorum ad eumque primorum est* $= (p-1)(q-1)$.

DEMONSTRATIO

Cum numerus omnium numerorum ipso $n = pq$ minorum sit $pq - 1$, hinc primum ii debent excludi, qui per p sunt divisibiles, deinde vero etiam

ii, qui per q; hisque deletis relinquetur multitudo quaesita. Notentur ergo ab unitate usque ad pq numeri, qui sunt ad p primi, hoc modo:

$$\begin{array}{ccccc}
1, & 2, & 3, & 4, & \ldots\ p-1, \\
p+1, & p+2, & p+3, & p+4, & \ldots\ 2p-1, \\
2p+1, & 2p+2, & 2p+3, & 2p+4, & \ldots\ 3p-1, \\
3p+1, & 3p+2, & 3p+3, & 3p+4, & \ldots\ 4p-1, \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
(q-1)p+1, & (q-1)p+2, & (q-1)p+3, & (q-1)p+4, & \ldots\ pq-1
\end{array}$$

atque iam ex his ii tantum eligi debent, qui simul quoque ad q sunt primi. Considerentur ergo series verticales, quarum numerus est $p-1$; quaelibet autem continet q terminos in arithmetica progressione crescentes differentia existente p, quae est ad q numerus primus. In qualibet ergo serie verticali omnes termini praeter unum ad q erunt primi (per § 7); unde unaquaeque series verticalis continet $q-1$ numeros ad q primos. Quare cum numerus serierum verticalium sit $p-1$, in omnibus continentur simul $(p-1)(q-1)$ numeri ad q primi iidemque igitur etiam ad productum pq erunt primi; consequenter inter omnes numeros ipso pq minores reperientur $(p-1)(q-1)$ numeri ad pq primi. Q. E. D.

COROLLARIUM 1

17. Cum multitudo omnium numerorum ipso producto pq minorum sit $pq-1$, inter eos semper sunt $(p-1)(q-1) = pq-p-q+1$ primi ad pq, reliqui vero, quorum numerus est $p+q-2$, ad eum sunt compositi seu cum eo communem habent divisorem vel p vel q.

COROLLARIUM 2

18. Hoc etiam inde patet, quod inter numeros ipso producto pq minores sint $q-1$ numeri per p divisibiles, scilicet

$$p,\quad 2p,\quad 3p,\quad 4p,\quad \ldots\ (q-1)p,$$

deinde inter eosdem sunt $p-1$ numeri per q divisibiles, nempe

$$q, \quad 2q, \quad 3q, \quad 4q, \ldots (p-1)q;$$

qui cum ab illis omnes sint diversi, omnino habentur

$$(q-1)+(p-1)=p+q-2$$

numeri, qui ad pq non sunt primi.

COROLLARIUM 3

19. Si ergo quaeratur, quot ab 1 usque ad 15 sint numeri ad 15 primi, ob $p=3$ et $q=5$ regula docet eorum numerum esse $2\cdot 4=8$, quippe qui sunt

$$1, 2, 4, 7, 8, 11, 13, 14.$$

Simili modo ab 1 ad 35 ob $p=5$ et $q=7$ multitudo numerorum ad 35 primorum est $4\cdot 6=24$ hique numeri sunt

$$1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29,$$
$$31, 32, 33, 34.$$

SCHOLION

20. Quoniam hic quaestio est de numeris, qui ad quempiam numerum sint primi eoque minores, eos commode *partes* ad istum numerum *primas* appellare licebit. Ita si numerus propositus fuerit primus $=p$, numerus partium ad eum primarum est $=p-1$; si numerus propositus sit potestas quaecunque numeri primi $=p^n$, numerus partium ad eum primarum erit $=p^n-p^{n-1}=p^{n-1}(p-1)$; at si numerus propositus sit productum duorum numerorum primorum disparium $=pq$, numerus partium ad eum primarum est $=(p-1)(q-1)$; hocque modo ambages in loquendo contrahemus. Simili modo demonstrare possemus, si numerus propositus sit productum ex tribus numeris primis disparibus $=pqr$, numerum partium ad eum primarum fore $=(p-1)(q-1)(r-1)$; hocque adeo ad productum plurium extendere liceret. Verum sequens propositio omnes hos casus in se complectetur.

THEOREMA 5

21. *Si sint A et B numeri inter se primi et numerus partium ad A primarum sit $=a$, numerus vero partium ad B primarum sit $=b$, tum numerus partium ad productum AB primarum erit $=ab$.*

DEMONSTRATIO

Sint $1, \alpha, \beta, \gamma, \ldots \omega$ numeri illi ipso A minores ad eumque primi seu partes ad A primae, quarum igitur partium numerus per hypothesin est $=a$. Totidem ergo erunt numeri ad A, itidem primi erunt ab A ad $2A$, item a $2A$ ad $3A$, et ita porro. Hoc modo exhiberi poterunt omnes numeri ad A primi ab unitate usque ad numerum propositum AB, quos sequens schema exhibebit:

$$\begin{array}{ccccc}
1, & \alpha, & \beta, & \ldots & \omega, \\
A+1, & A+\alpha, & A+\beta, & \ldots & A+\omega, \\
2A+1, & 2A+\alpha, & 2A+\beta, & \ldots & 2A+\omega, \\
3A+1, & 3A+\alpha, & 3A+\beta, & \ldots & 3A+\omega, \\
\vdots & \vdots & \vdots & & \vdots \\
(B-1)A+1, & (B-1)A+\alpha, & (B-1)A+\beta, & \ldots & (B-1)A+\omega.
\end{array}$$

Hic singulae series horizontales continent a terminos numerusque omnium serierum horizontalium est $=B$, unde omnes series iunctim offerunt aB terminos, qui iam omnes ad A erunt primi. Inde ergo adhuc excludi debent ii, qui ad B non sunt primi, ut hoc modo relinquantur, qui non solum ad A, sed etiam ad B ideoque ad ipsum productum AB sint primi; seu ex his seriebus ii tantum termini numerari debent, qui etiam ad B sint primi. Hunc in finem consideremus series verticaliter; et cum numerus serierum verticalium sit $=a$, quaelibet series verticalis continebit B terminos in arithmetica progressione auctos; quorum differentia cum sit $=A$ ideoque numerus ad B primus, per Theorema 2 quaelibet series verticalis tot continebit terminos ad B primos, quot dantur partes ad numerum B primae; eorum ergo numerus est per hypothesin $=b$. Cum igitur singulae series verticales con-

tineant b terminos ad B primos, qui propterea etiam erunt ad productum AB primi, numerus omnium terminorum ad AB primorum, hoc est partium ad hunc numerum AB primarum, erit $= ab$. Q. E. D.

COROLLARIUM 1

22. Si insuper tertius numerus C adiiciatur, qui sit ad utrumque praecedentium A et B seu ad eorum productum AB primus, et numerus partium ad C primarum sit $= c$, tum numerus partium ad productum ABC primarum erit $= abc$. Productum enim AB considerari potest tanquam unus numerus, cuius partium ad eum primarum multitudo sit $= ab$; et quia C ad AB est primus, Theorema hic habet locum.

COROLLARIUM 2

23. Cum igitur unusquisque numerus N resolvi possit in factores inter se primos, qui singuli sint vel ipsi numeri primi vel potestates primorum, ope huius regulae multitudo partium ad numerum quemcunque N primarum assignari poterit.

COROLLARIUM 3

24. Existentibus scilicet p, q, r, s etc. numeris primis omnis numerus N in huiusmodi forma $N = p^\lambda q^\mu r^\nu s^\xi$ comprehendetur, unde numerus partium ad N primarum erit

$$p^{\lambda-1}(p-1)\cdot q^{\mu-1}(q-1)\cdot r^{\nu-1}(r-1)\cdot s^{\xi-1}(s-1).$$

COROLLARIUM 4

25. Pro formis igitur numerorum simplicioribus multitudo partium ad eos primarum ita se habebit:

Numerus propositus	Multitudo partium ad eum primarum
p	$p-1$
pp	$p(p-1)$
pq	$(p-1)(q-1)$
p^3	$pp(p-1)$
p^2q	$p(p-1)(q-1)$
pqr	$(p-1)(q-1)(r-1)$
p^4	$p^3(p-1)$
p^3q	$p^2(p-1)(q-1)$
p^2q^2	$p(p-1)q(q-1)$
p^2qr	$p(p-1)(q-1)(r-1)$
$pqrs$	$(p-1)(q-1)(r-1)(s-1)$
p^5	$p^4(p-1)$
p^4q	$p^3(p-1)(q-1)$
p^3q^2	$p^2(p-1)q(q-1)$
p^3qr	$p^2(p-1)(q-1)(r-1)$
p^2q^2r	$p(p-1)q(q-1)(r-1)$
p^2qrs	$p(p-1)(q-1)(r-1)(s-1)$
$pqrst$	$(p-1)(q-1)(r-1)(s-1)(t-1)$

Numerus propositus	Multitudo partium ad eum primarum
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8
21	12
22	10
23	22
24	8
25	20

COROLLARIUM 5

26. Hinc igitur proposito numero quocunque multitudo partium ad eum primarum expedite definietur. Veluti si proponatur 360, cum sit $360 = 2^3 \cdot 3^2 \cdot 5$, erit multitudo partium ad 360 primarum $= 4 \cdot 6 \cdot 4 = 96$.

SCHOLION

27. Haec circa multitudinem partium ad numerum quemvis primarum pro praesenti instituto sufficere possunt. Interim tamen circa ipsas partes ad

quemvis numerum primas haec notasse iuvabit: Si numerus propositus fuerit N atque inter partes ad eum primas occurrat numerus α, ibidem quoque occurret numerus $N-\alpha$, quoniam existente α ad N primo etiam $N-\alpha$ erit ad N primus. Hinc pro quovis numero partes tantum eius semisse minores invenisse sufficiet, cum reliquae sint earum complementa ad ipsum numerum N. Simili modo, si N sit numerus par, inter partes ad N primas etiam occurret $\frac{1}{2}N-\alpha$, tum etiam $\frac{1}{2}N+\alpha$.[1]) Item si N sit divisibilis per numerum quemcunque n, inter partes ad eum primas quoque occurrent hi numeri[1])

$$\frac{1}{n}N\pm\alpha,\quad \frac{2}{n}N\pm\alpha,\quad \frac{3}{n}N\pm\alpha,\ldots \frac{n-1}{n}N\pm\alpha \quad \text{et} \quad N-\alpha$$

hincque multo facilius ipsae partes istae actu exhiberi poterunt.

THEOREMA 6[2])

28. *Si numerus x fuerit primus ad N, tum omnes potestates ipsius x per N divisae relinquent residua, quae erunt ad numerum N prima.*

DEMONSTRATIO

Cum enim x sit numerus ad N primus, omnes eius potestates erunt quoque ad N primae, ideoque si per N dividantur, residua etiam ad N erunt numeri primi. Q. E. D.

COROLLARIUM 1

29. Inter residua ergo potestatum ipsius x per N divisarum alii numeri non occurrunt, nisi qui sint partes ad N primae; quarum numerus cum sit pro indole numeri N determinatus, innumerabiles existent potestates ipsius x, quae per N divisae aequalia relinquunt residua.

1) Haec theoremata ad numeros compositos spectantia falsa esse neque nisi pro peculiaribus numeris N et n valere satis demonstrant exempla

$$\frac{6}{2}-1=2,\quad \frac{6}{2}+1=4,\quad \frac{12}{4}-1=2,\quad \frac{12}{4}+1=4,\quad \frac{18}{2}-1=8,\quad \frac{18}{2}+1=10,$$

$$\frac{20}{5}+1=5,\quad \frac{2}{5}\cdot 20-3=5,\quad \frac{60}{3}+1=21,\quad \frac{60}{3}-11=9,\quad \frac{2}{3}\cdot 60+11=51 \text{ etc.}$$ F. R.

2) Confer ad disquisitiones sequentes Commentationem 262 huius voluminis F. R.

COROLLARIUM 2

30. Inter residua autem ista ex divisione potestatum ipsius x per numerum N orta semper reperietur unitas, propterea quod inter potestates ipsius x etiam referri debet $x^0 = 1$. Utrum autem praeter unitatem etiam omnes reliquae partes ad N primae inter residua occurrant necne, mox videbimus.

COROLLARIUM 3

31. Si pro x capiatur unitas, omnia residua erunt unitates, quicunque numerus pro N fuerit assumtus. Deinde si sumatur $x = N - 1$, qui numerus ad N etiam est primus, in residuis ex divisione potestatum $(N-1)^0$, $(N-1)^1$, $(N-1)^2$, $(N-1)^3$ etc. ortis nonnisi duo reperientur diversa, scilicet 1 et $N-1$, quae continuo se alternatim excipiunt.

COROLLARIUM 4

32. Prout igitur numerus x ratione ad N fuerit comparatus, utique fieri potest, ut inter residua omnium potestatum ipsius x non omnes partes ad divisorem N primae occurrant.

COROLLARIUM 5

33. Si ergo omnes partes ad numerum N primae sint $1, a, b, c, d, e, \ldots$, quarum numerus sit $= n$, inter residua memorata vel omnes istae partes occurrent vel quaedam tantum, inter quas autem semper unitas reperietur.

COROLLARIUM 6

34. Quodsi non omnes illae partes in residuis ex divisione potestatum ipsius x per numerum N relictis occurrant, illae partes in duas classes distribuentur, quarum altera continebit partes in residuis occurrentes, altera vero partes in residuis non occurrentes.

THEOREMA 7

35. *Si series potestatum x^0, x^1, x^2, x^3, x^4, x^5 etc. per numerum N, qui ad x sit primus, dividatur, eousque residua prodibunt diversa, donec perveniatur ad potestatem, quae iterum unitatem pro residuo praebeat.*

DEMONSTRATIO

Quoniam serie potestatum $1, x, x^2, x^3, x^4$ etc. in infinitum continuata omnia residua diversa esse nequeunt, necesse est, ut tandem quodpiam ex praecedentibus redeat; ac dico unitatem esse id residuum, quod omnium primum sit rediturum. Quod si quis neget, sit x^μ ea potestas, cuius residuum primum in sequentibus ex potestate $x^{\mu+\nu}$ redeat; cum igitur potestates x^μ et $x^{\mu+\nu}$ aequalia praebeant residua, earum differentia $x^{\mu+\nu} - x^\mu = x^\mu(x^\nu - 1)$ per numerum N erit divisibilis. Verum producti $x^\mu(x^\nu - 1)$ factor prior ad N est numerus primus, ergo alter $x^\nu - 1$ per N divisibilis sit necesse est. Hinc autem potestas x^ν per N divisa residuum daret $=1$ sicque unitas inter sequentia residua citius redibit quam residuum potestatis x^μ, quippe quod per hypothesin demum in potestate altiore $x^{\mu+\nu}$ recurrit. Ex quo evidens nullum residuum iterum occurrere posse, nisi ante unitas inter residua redierit. Q. E. D.

COROLLARIUM 1

36. Postquam divisio terminorum seriei $1, x, x^2, x^3, x^4$ etc. per numerum N ad x primum ab initio dedit residua diversa, puta $1, \alpha, \beta, \gamma$ etc., tandem iterum occurret primum residuum 1; quod si oriatur ex potestate x^ν, numerus praecedentium residuorum diversorum erit $=\nu$.

COROLLARIUM 2

37. Quando autem potestas x^ν residuum dat 1, idem, quod primus terminus x^0, potestas sequens $x^{\nu+1}$ idem dabit residuum, quod x^1; et sequentium quaecunque $x^{\nu+\mu}$ idem, quod potestas x^μ. Cum enim differentia $x^{\nu+\mu} - x^\mu = x^\mu(x^\nu - 1)$ sit divisibilis per N, necesse est, ut ambo termini $x^{\nu+\mu}$ et x^μ per N divisi idem praebeant residuum.

COROLLARIUM 3

38. Cum post potestatem x^ν eadem residua $1, \alpha, \beta, \gamma$ etc. ordine recurrant, potestas $x^{2\nu}$ similique modo post eam potestates $x^{3\nu}, x^{4\nu}, x^{5\nu}$ etc. omnes per N divisae idem residuum 1 relinquent. Quin etiam omnes potestates $x^\mu, x^{\mu+\nu}, x^{\mu+2\nu}, x^{\mu+3\nu}, x^{\mu+4\nu}$ etc. aequalia residua suppeditabunt.

COROLLARIUM 4

39. Si igitur x^ν fuerit infima potestas, quae post $x^0 = 1$ iterum unitatem pro residuo praebeat, numerus diversorum residuorum erit ν. Cum ergo numerus partium ad numerum N primarum sit $= n$, fieri certe nequit, ut sit $\nu > n$; erit ergo vel $\nu = n$ vel $\nu < n$.

COROLLARIUM 5

40. Si ergo series potestatum $1, x, x^2, x^3$ etc. usque ad x^n continuetur, inter eas certe una saltem reperietur praeter primum terminum 1, quae per N divisa unitatem relinquat. Plures fortasse huiusmodi potestates aliquando, sed pauciores una nunquam existent.

SCHOLION

41. Residua proprie semper sunt numeri minores divisore N, sed nihil impedit, quominus numeros etiam maiores tanquam residua spectemus, cuiusmodi relinquuntur, si quotus nimis parvus accipiatur. Ita si in divisione cuiuspiam numeri per N relinquatur $N + \alpha$, hoc residuum aequivalens ipsi α censeri debet; hincque, si de residuis sermo sit, omnes hi numeri α, $N + \alpha$, $2N + \alpha$, $3N + \alpha$ etc. instar unius residui α sunt considerandi. Scilicet multipla quaecunque divisoris N sive adiecta sive demta a quopiam residuo α eius naturam non mutant atque hoc modo etiam numeri negativi commode inter residua referuntur; veluti $\alpha - N$ pro eodem residuo est habendum ac α et residuum -1 aequivalet residuo $N - 1$. Ex his conficitur omnes numeros, qui per N divisi idem exhibeant residuum α, pro eodem residuo haberi posse; ex quo enim numero per divisionem quotum nimis parvum sumendo oritur residuum vel $N + \alpha$ vel $2N + \alpha$ vel $3N + \alpha$ etc., ex eodem quotum plenum sumendo nascitur residuum α; tum vero indidem, si quotus capiatur nimis magnus, obtinebuntur residua negativa $\alpha - N$ vel $\alpha - 2N$ vel $\alpha - 3N$ etc., quae ergo etiam ab α non discrepare sunt censenda.

THEOREMA 8

42. *Si, dum termini progressionis* $1, x, x^2, x^3, x^4$ *etc. per numerum* N *ad* x *primum dividantur, residua fuerint* $1, a, b, c$ *etc., in iisdem quoque occurrent tam singulorum omnes potestates quam producta quaecunque vel binorum vel ternorum vel quotlibet in se multiplicatorum.*

DEMONSTRATIO

Nascantur residua a, b, c etc. ex potestatibus x^α, x^β, x^γ etc. ac numeros etiam maiores quam N in residuis admittendo ex potestatibus $x^{2\alpha}$, $x^{3\alpha}$, $x^{4\alpha}$ etc. orientur residua a^2, a^3, a^4 etc., quae igitur etiam in serie residuorum 1, a, b, c etc. continebuntur. Tum vero potestates $x^{\alpha+\beta}$, $x^{\alpha+\gamma}$, $x^{\alpha+\beta+\gamma}$ etc. relinquent residua ab, ac, abc etc., quae ergo etiam in serie residuorum inveniri debebunt. Producta igitur quomodocunque ex residuis 1, a, b, c etc. per multiplicationem formata omnia in eadem serie residuorum occurrent, siquidem singula per ablationem divisoris N, quoties id fieri potest, ad minimam formam reducantur. Q. E. D.

COROLLARIUM 1

43. Haec indoles residuorum eo clarius eluceret, si eorum loco ipsae illae potestates ipsius x, unde sunt orta, substituantur; tum enim manifesto non solum omnes potestates harum potestatum, sed etiam earum producta quaecunque in residuis occurrunt.

COROLLARIUM 2

44. Neque tamen ideo numerus residuorum indeterminatus evadit; quemadmodum enim iam vidimus ex innumeris potestatibus paria residua provenire, ita, si omnia haec residua ex mutua multiplicatione nata ad formam minimam reducantur, ad multitudinem modicam revocabuntur.

COROLLARIUM 3

45. Ita si minima potestas, quae per N divisa iterum unitatem relinquit, fuerit x^ν, ita ut numerus residuorum 1, a, b, c etc. sit $=\nu$, tum in eodem numero omnia producta ex multiplicatione numerorum a, b, c etc. nata continebuntur, siquidem ab iis divisor N toties, quoties fieri potest, auferatur.

SCHOLION

46. Unicum exemplum omnibus dubiis, quae forte circa hanc apparentem residuorum multitudinem nasci possunt, solvendis sufficiet. Sit igitur $x=2$ et pro divisore sumatur $N=15$, qui scilicet ad 2 sit primus; iam singulae binarii potestates per 15 divisae sequentia relinquent residua:

Potestates	1,	2,	2^2,	2^3,	2^4,	2^5,	2^6,	2^7,	2^8,	2^9,	2^{10}	etc.
residua	1,	2,	4,	8,	1,	2,	4,	8,	1,	2,	4	etc.

Potestas igitur, quae primum unitatem reproducit, est 2^4, a qua residua continuo eodem ordine 1, 2, 4, 8 repetuntur, ita ut tantum quaterna residua diversa occurrant. Hic iam manifestum est, quomodocunque haec residua in se invicem multiplicentur, nunquam numeros inde produci, qui non in eodem quaternione includantur, postquam scilicet ablatione divisoris 15 ad formam minimam fuerint revocata. In hoc quoque exemplo inter residua non omnes partes ad 15 primae occurrunt, sed inde excluduntur istae partes 7, 11, 13, 14, quae pariter ad 15 sunt primae; unde distributio supra [§ 34] facta inter partes ad divisorem primas, quae in residuis occurrunt et quae non occurrunt, illustratur, ad quam potissimum in sequentibus probe respiciatur.

THEOREMA 9

47. *In residuis ex divisione potestatum cuiuspiam numeri per divisorem ad eum primum relictis vel omnes partes ad divisorem primae occurrunt vel numerus partium non occurrentium aequalis erit vel rationem tenebit multiplam ad numerum partium, quae residua constituunt.*

DEMONSTRATIO

Sit series potestatum 1, x, x^2, x^3, x^4, x^5 etc. et divisor N ad x primus, cuius partium ad ipsum primarum numerus sit $= n$. Sit porro x^ν minima potestas, quae per N divisa iterum unitatem relinquit, ita ut numerus omnium diversorum residuorum sit $= \nu$; quae cum omnia sint ad N numeri primi, eorum numerus erit vel $= n$ vel minor; priorique casu inter residua utique omnes partes ad N primae occurrent.

Consideremus igitur casum, quo $\nu < n$, sintque

$$1,\ a,\ b,\ c,\ d \text{ etc.}$$

omnia residua ex divisione potestatum

$$1,\ x,\ x^2,\ x^3,\ x^4, \ldots x^{\nu-1}$$

per divisorem N relicta; quorum numerus cum sit $= \nu$, non omnes partes

ad N primae ibi occurrent. Sit igitur α huiusmodi pars in residuis non occurrens ac demonstrari potest nullum quoque horum numerorum

$$\alpha a,\ \alpha b,\ \alpha c,\ \alpha d \text{ etc.}$$

in residuis occurrere. Nam si αa esset residuum potestati x^λ respondens, quia a est quoque residuum ex quapiam potestate, puta x^ζ, ortum, foret $x^\lambda = AN + \alpha a$ et $x^\zeta = BN + a$ ideoque $x^\lambda - \alpha x^\zeta = (A - \alpha B)N$ per N divisibile. Cum autem x^ζ ad N sit numerus primus et $x^\lambda - \alpha x^\zeta = x^\zeta(x^{\lambda-\zeta} - \alpha)$, numerus $x^{\lambda-\zeta} - \alpha$ esset per N divisibilis sicque potestas $x^{\lambda-\zeta}$ per N divisa relinqueret residuum α contra hypothesin. Cum igitur α, αa, αb, αc etc., quorum numerus est $=\nu$, sint numeri ad N primi atque divisione per N ad partes ad N primas revocari possint, statim atque una pars α ad N prima in residuis non reperitur, simul quoque ν eiusmodi partes assignari possunt in residuis non occurrentes. Numerus ergo partium non occurrentium, nisi sit nullus, ad minimum est $=\nu$, ac si praeterea fuerit pars ad N prima β in his non-residuis non contenta, denuo habebuntur ν partes novae in residuis non occurrentes, sicque porro. Quare si non omnes partes ad divisorem N primae in residuis occurrant, numerus partium non occurrentium necessario est vel $=\nu$ vel $=2\nu$ vel $=3\nu$ vel alii cuipiam multiplo ipsius ν, hoc est numeri diversorum residuorum. Q. E. D.

COROLLARIUM 1

48. Constituto ergo discrimine inter partes ad divisorem N primas eas, quae sunt residua, et eas, quae non sunt residua, ex demonstratione patet productum ex residuo et non-residuo in classe non-residuorum semper contineri. Ita si a sit residuum, α non-residuum, productum αa certe non erit residuum.

COROLLARIUM 2

49. Contra autem iam supra vidimus productum ex duobus pluribusve residuis in classe residuorum reperiri. Unde sequitur productum ex uno non-residuo et quotcunque residuis in classe non-residuorum occurrere debere.

SCHOLION

50. Vis huius demonstrationis isto nititur fundamento, quodsi inter residua occurrant partes 1, a, b, c, d etc. ad divisorem primae atque α

fuerit etiam pars ad divisorem prima in his residuis non contenta, tum producta omnia αa, αb, αc, αd etc. non solum in residuis non occurrere, quod quidem perfecte est demonstratum, sed etiam ea esse partes ad divisorem N primas omnesque inter se diversas seu, si ea per N actu dividantur, relinqui residua diversa. Illud quidem per se est perspicuum; cum enim tam α quam a, b, c, d etc. sint numeri ad N primi, etiam eorum producta ad N prima sint necesse est. Quod autem producta αa, αb, αc, αd etc. sint omnia ad N relata inter se diversa, intelligitur, quod, si verbi gratia duo αa et αb per N divisa paria darent residua, eorum differentia $\alpha b - \alpha a = \alpha(b-a)$ per N esset divisibilis ideoque et $b-a$; id quod hypothesi, quod a et b sint diversae partes ad N primae, repugnat.

THEOREMA 10

51. *Exponens minimae potestatis x^ν, quae per numerum N ad x primum divisa unitatem relinquit, vel est aequalis numero partium ad N primarum vel huius numeri semissis aliave eius pars aliquota.*

DEMONSTRATIO

Sit n numerus partium ad N primarum; quarum cum ν constituant residua, erit numerus non-residuorum $= n - \nu$. Vidimus autem hunc numerum esse vel $= 0$ vel $= \nu$ vel $= 2\nu$ vel alii cuipiam multiplo exponentis ν. Sit ergo $n - \nu = (m-1)\nu$, ita ut m denotet vel unitatem vel alium quemvis numerum integrum, atque hinc obtinebimus $n = m\nu$ et $\nu = \frac{n}{m}$; unde patet exponentem minimae potestatis ipsius x, quae per N divisa unitatem relinquit, esse vel $= n$, si $m = 1$, vel $= \frac{n}{2}$, si $m = 2$, vel in genere esse partem quampiam aliquotam numeri n, qui exprimit multitudinem partium ad divisorem N primarum. Q. E. D.

COROLLARIUM 1

52. Si x^ν fuerit minima potestas, quae per numerum N ad x primum divisa unitatem relinquit, sequentes potestates idem residuum relinquentes sunt $x^{2\nu}$, $x^{3\nu}$, $x^{4\nu}$, $x^{5\nu}$ etc. neque praeterea ullae aliae dantur, quae per N divisae unitatem relinquant.

COROLLARIUM 2

53. Exponens ergo huius potestatis minimae semper cum numero partium ad divisorem N primarum ita connectitur, ut sit vel illi ipsi vel cuipiam eius parti aliquotae aequalis.

SCHOLION

54. Quo haec ratio clarius perspiciatur, iuvabit nonnullos casus simpliciores perpendisse. Sit igitur $x = 2$ et pro N sumamus successive numeros impares utpote ad $x = 2$ primos atque exhibeamus minimam potestatem binarii, quae per quemque numerum imparem divisa unitatem relinquat.

Divisor N	Numerus partium ad eum primarum n	Minima potestas 2^ν, quae per N divisa unitatem relinquit	
3	2	2^2	ergo $\nu = n$
5	4	2^4	„ $\nu = n$
7	6	2^3	„ $\nu = \frac{1}{2} n$
9	6	2^6	„ $\nu = n$
11	10	2^{10}	„ $\nu = n$
13	12	2^{12}	„ $\nu = n$
15	8	2^4	„ $\nu = \frac{1}{2} n$
17	16	2^8	„ $\nu = \frac{1}{2} n$
19	18	2^{18}	„ $\nu = n$
21	12	2^6	„ $\nu = \frac{1}{2} n$
23	22	2^{11}	„ $\nu = \frac{1}{2} n$
25	20	2^{20}	„ $\nu = n$
27	18	2^{18}	„ $\nu = n$
29	28	2^{28}	„ $\nu = n$
31	30	2^5	„ $\nu = \frac{1}{6} n$

THEOREMA 11

55. *Si fuerit N ad x numerus primus et n numerus partium ad N primarum, tum potestas x^n unitate minuta semper per numerum N erit divisibilis.*[1])

DEMONSTRATIO

Sit enim x^ν minima potestas, quae per N divisa unitatem relinquit, eritque ν vel aequalis ipsi numero n vel parti eius cuipiam aliquotae $\frac{n}{m}$. Cum igitur $x^\nu - 1$ per N sit divisibilis, quia forma $x^{\nu m} - 1$ factorem habet $x^\nu - 1$, etiam ista forma $x^{\nu m} - 1$ seu $x^n - 1$ per N erit divisibilis. Q. E. D.

COROLLARIUM 1

56. Si ergo divisor N sit numerus primus p neque x per p sit divisibilis, tum semper numerus $x^{p-1} - 1$ per numerum primum p erit divisibilis, uti quidem dudum[2]) demonstravi.

COROLLARIUM 2

57. Si praeterea p, q, r etc. sint numeri primi neque x ullum eorum implicet, ex hoc theoremate sequitur

has formas	fore divisibiles per
$x^{p-1} - 1$	p
$x^{p(p-1)} - 1$	pp
$x^{(p-1)(q-1)} - 1$	pq
$x^{pp(p-1)} - 1$	p^3
$x^{p(p-1)(q-1)} - 1$	ppq
$x^{(p-1)(q-1)(r-1)} - 1$	pqr.

1) Casus speciales huius theorematis generalis, quod in se complectitur uti casum specialissimum celebre illud theorema FERMATIANUM (vide paragraphum sequentem), EULERUS iam in prima Commentatione huius voluminis proposuit. F. R.

2) Vide notam p. 534. F. R.

COROLLARIUM 3

58. Si x et y sint primi ad divisorem N, cuius partium ad eum primarum numerus sit $= n$, quia tam $x^n - 1$ quam $y^n - 1$ est divisibilis per N, erit etiam $x^n - y^n$ semper divisibilis per numerum N, quod est Theorema generalius.

COROLLARIUM 4

59. Proposito ergo numero quocunque N, cuius partium ad ipsum primarum numerus sit $= n$, quicunque numerus ad N primus pro x capiatur, formula $x^n - 1$ semper erit per numerum N divisibilis.

COROLLARIUM 5

60. Saepenumero vero etiam evenire potest, ut huiusmodi formula simplicior, veluti $x^{\frac{1}{2}n} - 1$ vel $x^{\frac{1}{3}n} - 1$ vel $x^{\frac{1}{4}n} - 1$ etc., sit per numerum N divisibilis, quae circumstantia pendet a certa indole numeri x.[1])

SCHOLION

61. En ergo novam demonstrationem Theorematis FERMATIANI, quod, si fuerit p numerus primus, omnes numeri in hac forma $a^{p-1} - 1$ contenti sint per p divisibiles, dummodo numerus a non sit per p divisibilis. Duas[2]) autem iam dudum huius Theorematis dederam demonstrationes, sed ea, quam hic exhibui, iis praestare videtur, quod non solum ad numeros primos adstringitur. Quicunque enim numerus N pro divisore accipiatur, dummodo a ad eum sit primus, hic numerus $a^n - 1$ semper per N erit divisibilis, siquidem n denotet numerum partium ad N primarum, quae propositio multo latius patet quam FERMATIANA. Ex quo eo magis utilitas Theorematum primorum elucet, quibus numerum partium ad quemque numerum primarum definivi, quae sine hac applicatione nimis sterilia videri potuissent.

---

1) Vide etiam observationem „haud inelegantem", quae invenitur sub finem Summarii p. 532. F. R.

2) Sed vide notam p. 534. F. R.

SUPPLEMENTUM QUORUNDAM THEOREMATUM ARITHMETICORUM QUAE IN NONNULLIS DEMONSTRATIONIBUS SUPPONUNTUR

Commentatio 272 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 8 (1760/1), 1763, p. 105—128
Summarium ibidem p. 18—20

SUMMARIUM

Versantur haec Theoremata circa numeros, qui sunt aggregata ex quadrato et triplo alterius quadrati formata ideoque hac formula generali $pp + 3qq$ continentur. Scilicet si duae series constituantur, quarum altera constet ex numeris quadratis, altera ex iisdem triplicatis, uti

I. 1, 4, 9, 16, 25, 36, 49, 64, 81,
II. 3, 12, 27, 48, 75, 108, 147, 192, 243,

atque singuli prioris seriei singulis posterioris seriei addantur, oriuntur ii numeri, quorum indoles hic consideratur et qui secundum ordinem magnitudinis dispositi sunt ad centum usque

4, 7, 12, 13, 16, 19, 21, 28, 31, 36, 37, 39, 43, 48, 49,
52, 57, 61, 63, 64, 67, 73, 76, 79, 84, 91, 93, 97, 100.

Hinc si primo excerpantur numeri, qui sunt primi,

7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97,

hi omnes unitate minuti per 6 divisibiles deprehenduntur seu in formula $6n + 1$ continentur, cuius quidem ratio facile perspicitur, cum ex forma $pp + 3qq$ alii numeri primi oriri nequeant, nisi qui per 3 divisi unitatem relinquant. Sed eius inversum, quod vicissim

omnes numeri primi istius formae $6n+1$ simul in illo numerorum genere occurrant, veritas est multo magis ardua, cuius demonstratio maximas ambages postulat. Demonstrari scilicet oportet semper dari numeros p et q, ut sit $6n+1=pp+3qq$, siquidem numerus $6n+1$ fuerit primus; ubi imprimis notari convenit, nisi $6n+1$ sit primus, hanc proprietatem saepius fallere, uti fit in numeris 55, 85, qui etsi multiplum senarii unitate superant, tamen neutiquam in forma $pp+3qq$ continentur. At si huiusmodi numerus $6n+1$ fuerit primus, quantumvis sit magnus, veluti 20161, certo pronunciare licet duo dari quadrata pp et qq, ut sit $20161=pp+3qq$; reperitur autem $p=31$ et $q=80$ neque plus uno modo hoc fieri potest.

En ergo summam Theorematum hic singulari prorsus modo demonstratorum, quod omnis numerus primus formae $6n+1$ semper in hac forma $pp+3qq$, idque unico tantum modo, contineatur, ex quo sequitur, si quispiam numerus formae $6n+1$ vel prorsus non in forma $pp+3qq$ contineatur vel plus uno modo, tum eum certe non fore primum. Fundamentum autem harum demonstrationum in hac propositione est situm, quodsi numerus formae $pp+3qq$ non fuerit primus, eum non alios admittere divisores, nisi qui ipsi in eadem forma $pp+3qq$ contineantur.

His autem principiis Auctor iam olim erat usus, cum demonstrasset non dari duos cubos, quorum summa vel differentia sit cubus[1]), tum vero etiam nuper, cum nova plane methodo problema de tribus cubis inveniendis, quorum summa sit cubus, solvisset, quamobrem, ut hic nihil amplius desiderari posset, omnino necesse erat Theoremata ista rigidis demonstrationibus confirmari. Ceterum ingenue fatetur Auctor has demonstrationes ex principiis nimis alienis esse petitas fontesque magis proprios dari eo deducentes, ex quibus FERMATIUS hausisse videtur, cum inde se demonstravisse asseveret hanc aequationem generalem $a^n \pm b^n = c^n$ nunquam locum habere posse, statim atque exponens n binarium superet, cum tamen EULERUS hanc impossibilitatem tantum pro casibus $n=3$ et $n=4$ demonstrare valeat; ex quo eo magis dolendum est FERMATIANA inventa temporum iniuria periisse.[2])

Cum nuper demonstravissem non dari duos cubos, quorum summa sit cubus, sine sufficiente probatione assumseram omnes numeros in hac forma contentos $mm+mn+nn$, quae forma facile ad hanc reducitur $pp+3qq$, nunquam alios admittere divisores, nisi qui ipsi in eadem forma contineantur. Atque hinc conclusi, si forma $mm+mn+nn$ fuerit cubus aliave potestas, eius radicem quoque numerum eiusdem formae esse futuram; cui fun-

1) Sed vide notam 1 p. 558. F. R. 2) Vide notam 3 p. 574. F. R.

damento etiam tota demonstratio modo memorata innititur.[1]) Cum deinceps methodum novam et maxime generalem exposuissem tres cubos inveniendi, quorum summa sit cubus,[2]) quae simul omnibus adhuc usitatis facilitate longe praestabat, non solum eandem indolem numerorum in forma $mm + mn + nn$ seu $pp + 3qq$ contentorum tanquam certam assumsi, sed etiam in evolutione solutionis supposui huius generis numeros alios divisores primos praeter ternarium non implicare, nisi qui essent formae $6x + 1$.[3]) Quin etiam vicissim affirmare licet omnes numeros primos istius formae $6x + 1$, cuiusmodi sunt 7, 13, 19, 31, 37, 43 etc., ita esse comparatos, ut in forma $pp + 3qq$ contineantur,[4]) veluti

$$7 = 2^2 + 3 \cdot 1^2, \quad 13 = 1^2 + 3 \cdot 2^2, \quad 19 = 4^2 + 3 \cdot 1^2, \quad 31 = 2^2 + 3 \cdot 3^2 \quad \text{etc.}$$

Quae Theoremata etsi iam a FERMATIO[5]) fuerant prolata, nusquam tamen adhuc demonstrata reperiuntur; ex quo operae pretium me facturum putavi, si has assertiones rigidis demonstrationibus confirmarem, quo simul supra memoratae demonstrationes ad summum certitudinis gradum eveherentur.

His proprietatibus innituntur ratiocinia, quibus sum deductus ad tres cubos, quorum summa itidem est cubus; hinc autem omissis ratiociniis solutio consueto modo adornari poterit idoneis formis pro radicibus cuborum assumendis. Quarum ratio etsi non perspiciatur, tamen in hoc Analyseos genere problemata plerumque per huiusmodi formulas feliciter excogitatas resolvi solent, in quas saepenumero vel casu vel post plurima tentamina incidimus.

---

1) Talem demonstrationem EULERUS nunquam publicavit. Theorematis memorati demonstrationem aliis quidem fundamentis innitentem EULERUS nonnisi a. 1770 publici iuris fecit in libro, qui inscribitur *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, Zweyter Theil, zweyter Abschnitt, Cap. 15, § 243; *LEONHARDI EULERI Opera omnia*, series I, vol. 1. Vide etiam epistolas ab EULERO d. 4. Aug. 1753 et 17. Maii 1755 ad CHR. GOLDBACH datas, *Correspondance math. et phys. publiée par P. H. FUSS*, St.-Pétersbourg 1843, t. I, p. 614 et 621; *LEONHARDI EULERI Opera omnia*, series III. Vide praeterea G. ENESTROEM, Biblioth. Mathem. 9_3, 1908/9, p. 180. F. R.

2) Vide Commentationem 255 huius voluminis. F. R.

3) Hoc vero in Commentatione 255 nusquam supponitur. F. R.

4) Vide huius voluminis Commentationem 256, imprimis § 56, et Commentationem 164, imprimis theoremata 7—9 atque notam p. 194. F. R.

5) Vide FERMATII epistolam ad KENELMUM DIGBY scriptam, quae nota p. 466 laudata est. F. R.

Ita si tres cubi inveniri debeant, quorum summa sit cubus, positis eorum radicibus x, y et z statuatur

$$x^3 + y^3 + z^3 = v^3.$$

Tum vero istorum cuborum radicibus sequentes formae tribuantur

$$x = (m-n)p + qq, \qquad z = pp - (m+n)q,$$
$$y = (m+n)p - qq, \qquad v = pp + (m-n)q,$$

et quoniam loco quaternarum quantitatum x, y, z et v quaternae novae m, n, p et q in calculum introducuntur, his positionibus problema non restringi est censendum. Cum igitur vi problematis esse oporteat

$$x^3 + y^3 = v^3 - z^3$$

sive

$$(x+y)(xx - xy + yy) = (v-z)(vv + vz + zz),$$

per assumtas formas habebitur

$$x + y = 2mp, \quad xx - xy + yy = (mm + 3nn)pp - 6npqq + 3q^4,$$
$$v - z = 2mq, \quad vv + vz + zz = 3p^4 - 6nppq + (mm + 3nn)qq$$

hisque valoribus substitutis obtinebitur divisione utrinque per $2m$ facta

$$(mm + 3nn)p^3 - 6nppqq + 3pq^4 = 3p^4q - 6nppqq + (mm + 3nn)q^3;$$

ubi cum termini medii se utrinque destruant, fiet

$$(mm + 3nn)(p^3 - q^3) = 3p^4q - 3pq^4 = 3pq(p^3 - q^3).$$

Hic igitur commodo usu venit, ut haec aequatio per $p^3 - q^3$ dividi queat, in quo ipso summa utilitas nostrarum positionum consistit; nanciscimur enim hanc aequationem

$$mm + 3nn = 3pq,$$

unde assumtis numeris m et n cum altero reliquorum p vel q pro lubitu alter sponte et quidem rationaliter determinatur, quod eximium commodum non locum haberet, nisi postrema aequatio divisionem per $p^3 - q^3$ admisisset. Nisi ergo fractiones evitare velimus, habebimus statim

$$q = \frac{mm + 3nn}{3p}.$$

Verum etsi fractiones facile erui possunt, dum aeque multipla quaecunque radicum x, y, z et v pariter satisfaciunt, tamen ad expressiones simpliciores pertingemus, si numeros m et n statim ita assumamus, ut $mm+3nn$ primo divisibile evadat per 3, tum vero insuper duos contineat factores, quorum alter pro p, alter pro q accipi queat.

Primo igitur statuatur $m=3k$, ut fiat

$$pq=nn+3kk,$$

et quia, ut mox demonstrabo, numeri formae $nn+3kk$ alios non admittunt divisores, nisi qui ipsi sint eiusdem formae, ponamus

$$nn+3kk=(aa+3bb)(cc+3dd),$$

ut sit

$$p=aa+3bb \quad \text{et} \quad q=cc+3dd,$$

eritque vel

$$n=ac+3bd, \quad k=bc-ad, \quad m=3bc-3ad$$

vel

$$n=ac-3bd, \quad k=bc+ad, \quad m=3bc+3ad.$$

Hanc pluralitatem valorum per ambiguitatem signorum ita exhibere poterimus, ut sit

$$m=\pm 3(bc\pm ad), \qquad n=\pm(ac\mp 3bd),$$

ideoque diversi valores pro m et n sumtis pro a, b, c, d numeris quibuscunque erunt

I. $m+n=3(bc+ad)+(ac-3bd), \quad m-n=3(bc+ad)-(ac-3bd),$

II. $m+n=3(bc+ad)-(ac-3bd), \quad m-n=3(bc+ad)+(ac-3bd),$

III. $m+n=3(bc-ad)+(ac+3bd), \quad m-n=3(bc-ad)-(ac+3bd),$

IV. $m+n=3(bc-ad)-(ac+3bd), \quad m-n=3(bc-ad)+(ac+3bd).$

Hinc autem sequuntur solutiones, quas iam dudum fusius exposui, quare ad propositum revertor sequentes propositiones demonstraturus.

PROPOSITIO 1

1. *Si numeri a et b non sint numeri inter se primi, tum numerus $aa+3bb$ non erit primus, sed divisibilis erit per quadratum maximi communis divisoris numerorum a et b.*

DEMONSTRATIO

Sit enim m maximus communis divisor numerorum a et b, ita ut sit $a=mc$ et $b=md$ existentibus iam c et d numeris inter se primis, quia alioquin non esset maximus communis divisor. Ac numerus $aa+3bb$ induet hanc formam $mm(cc+3dd)$, quae propterea certo divisorem habet mm.

COROLLARIUM 1

2. Nisi ergo numeri a et b sint primi inter se, numerus ex iis formatus $aa+3bb$ primus esse nequit. Neque vero hinc vicissim concludere licet numerum $aa+3bb$ semper esse primum, quoties numeri a et b fuerint primi inter se.

COROLLARIUM 2

3. Primo autem patet numerum $aa+3bb$ divisibilem esse per ternarium, dum numerus a fuerit multiplum ternarii, etiamsi ceterum a et b fuerint numeri primi inter se. Neque vero unquam forma $aa+3bb$ per 9 altioremve ternarii potestatem est divisibilis, nisi ambo numeri a et b communem divisorem habeant 3.

COROLLARIUM 3

4. Deinde etiam patet formam $aa+3bb$ numerum parem esse non posse, nisi ambo numeri a et b vel sint pares vel impares. Utroque autem casu numerus $aa+3bb$ non solum per 2, sed etiam per 4 erit divisibilis.

COROLLARIUM 4

5. Non ergo datur numerus formae $aa+3bb$, qui sit impariter par, sed statim atque admittit divisorem 2, simul erit divisibilis per 4. Unde quoties

huiusmodi numeri fuerint pares, quaternarium tanquam eorum factorem simplicem considerare licet, etiamsi alias quaternarius utpote binarii quadratum non inter numeros primos referatur.

COROLLARIUM 5

6. Si ergo numerus formae $aa + 3bb$ sit primus, non solum certo constat ambos numeros a et b esse primos inter se, sed etiam utrumque non esse imparem. Necesse igitur est, ut alter sit par, alter vero impar.

PROPOSITIO 2

7. *Si numerus formae $aa + 3bb$ per ternarium est divisibilis, tunc etiam quotus est numerus formae eiusdem.*

DEMONSTRATIO

Si numerus $aa + 3bb$ per 3 est divisibilis, necesse est, ut radix prioris quadrati a sit multiplum ternarii. Ponamus ergo $a = 3c$ et numerus propositus erit $9cc + 3bb$, qui per 3 divisus dat quotum $3cc + bb$, qui utique est numerus eiusdem formae $aa + 3bb$.

SCHOLION

8. Notari hic convenit ipsum quoque ternarium esse numerum formae $aa + 3bb$, quippe qui prodit, si $a = 0$ et $b = 1$. Consideramus autem has duas formas $aa + 3bb$ et $mm + mn + nn$ tanquam aequivalentes, quoniam posterior in priorem transit ponendo $m = a + b$ et $n = b - a$; unde quicquid de altera demonstramus, etiam de altera valet. Posterior autem casu $m = 1$ et $n = 1$ manifesto dat 3. Videtur quidem forma $mm + mn + nn$, si numerorum m et n alter fuerit par, alter impar, ad priorem reduci non posse, quia tum in integris esse nequit $m = a + b$ et $n = b - a$; verum dantur adhuc aliae reductiones, scilicet $a = \frac{1}{2}m + n$ et $b = \frac{1}{2}m$ sive $a = m + \frac{1}{2}n$ et $b = \frac{1}{2}n$[1]), quarum ope, si numerorum m et n alter fuerit par, alter impar, forma $mm + mn + nn$ ad $aa + 3bb$ reducitur.

---

1) Editio princeps (atque etiam *Comment. arithm.*): *scilicet* $a = \frac{1}{2}m + n$, *et* $b = m$, *sive* $a = m + \frac{1}{2}n$, *et* $b = n$, *quarum ope* ... Sed vide etiam § 37. F. R.

PROPOSITIO 3

9. *Si numerus formae* $aa + 3bb$ *per quaternarium est divisibilis, tum etiam quotus erit numerus eiusdem formae* $aa + 3bb$.

DEMONSTRATIO

Divisio formae $aa + 3bb$ per 4 succedit, si vel uterque numerorum a et b fuerit par vel impar. Priori casu ponatur $a = 2c$ et $b = 2d$ fietque $aa + 3bb = 4cc + 12dd$, unde divisione per 4 instituta prodit quotus $cc + 3dd$.

Sin autem uterque numerus a et b fuerit impar, tum eorum vel summa vel differentia certo erit divisibilis per 4. Namque cum tam $a + b$ quam $a - b$ sit numerus par eorumque summa sit $2a$, hoc est numerus impariter par, necesse est, ut alter eorum sit impariter par, alter vero pariter par. Erit ergo vel $a + b = 4c$ vel $a - b = 4c$ ideoque $a = 4c \pm b$, quo valore substituto fiet

$$aa + 3bb = 16cc \pm 8bc + 4bb,$$

unde divisione per 4 instituta prodit quotus

$$4cc \pm 2bc + bb = (b \pm c)^2 + 3cc.$$

COROLLARIUM 1

10. Hic pariter notasse iuvabit ipsum quaternarium etiam esse numerum formae $aa + 3bb$ inde resultantem positis $a = 1$ et $b = 1$. At ex forma $mm + mn + nn$ quaternarius nascitur, si ponatur $n = 0$ et $m = 2$.

COROLLARIUM 2

11. Cum igitur viderimus dari numeros formae $aa + 3bb$, qui tam per 3 quam per 4 sint divisibiles, nunc demonstravimus quotos ex utraque divisione resultantes etiam esse numeros eiusdem formae $aa + 3bb$.

COROLLARIUM 3

12. Quodsi autem ambo numeri a et b fuerint impares, tum quotus ex divisione numeri $aa + 3bb$ per 4 nascens erit numerus impar. Vidimus enim quotum esse $4cc \pm 2bc + bb$, qui ob b numerum imparem certo est impar.

SCHOLION

13. Quod hactenus de divisione numerorum formae $aa+3bb$ per 3 et 4 demonstravimus, idem demonstrabimus de divisione per numerum quemcunque alium primum formae $aa+3bb$, quotum scilicet inde oriundum pariter fore numerum eiusdem formae. Hunc in finem, ut brevitati consulamus, denotabunt litterae P, Q, R, S etc. numeros primos formae $aa+3bb$, inter quos tamen etiam quaternarium referemus, etiamsi non sit primus, propterea quod binarius ab hac forma est excludendus.

PROPOSITIO 4

14. *Si numerus formae* $aa+3bb$ *est divisibilis per numerum primum* $P=pp+3qq$, *tum quotus est etiam numerus eiusdem formae.*

DEMONSTRATIO

Si $aa+3bb$ est divisibilis per $pp+3qq$, tum etiam $aapp+3bbpp$ per eundem est divisibilis itemque $aapp+3aaqq$, quare etiam horum numerorum differentia $3aaqq-3bbpp$ ideoque et

$$aaqq-bbpp=(aq+bp)(aq-bp).$$

Cum igitur $pp+3qq$ sit numerus primus, necesse est, ut alteruter istorum factorum, scilicet vel $aq+bp$ vel $aq-bp$, sit per $pp+3qq$ divisibilis. Ponatur ergo pro utroque casu

$$aq\pm bp=m(pp+3qq);$$

hincque fiet

$$a=\frac{m(pp+3qq)}{q}\mp\frac{bp}{q}=3mq+\frac{p}{q}(mp\mp b).$$

Verum quia a est numerus integer et p et q numeri inter se primi, necesse est, ut $mp\mp b$ divisionem per q admittat. Ponatur ergo $mp\mp b=\mp nq$ eritque

$$b=\pm mp+nq \quad \text{et} \quad a=3mq\mp np.$$

Cum igitur numeri a et b necessario hoc modo exprimantur, siquidem numerus

$aa+3bb$ per $pp+3qq$ fuerit divisibilis, hinc obtinebimus

$$aa+3bb=3mmpp+9mmqq+3nnqq+nnpp=(pp+3qq)(nn+3mm),$$

unde patet hunc numerum per numerum primum $P=pp+3qq$ divisum pro quoto dare $nn+3mm$, hoc est numerum formae $aa+3bb$.

COROLLARIUM 1

15. Quoties ergo numerus formae $aa+3bb$ divisorem primum habet $P=pp+3qq$, quotus est numerus formae $nn+3mm$. Vel, quod eodem redit, si numerus $aa+3bb$ constet duobus factoribus, quorum alter sit primus $P=pp+3qq$, tum etiam alter factor, sive sit numerus primus sive compositus, erit numerus formae $nn+3mm$.

COROLLARIUM 2

16. Si igitur numerus $aa+3bb$ duobus constaret factoribus, quorum alter non in forma $nn+3mm$ contineretur, tum alter certe non erit primus formae $pp+3qq$.

COROLLARIUM 3

17. Ex demonstratione patet, quomodo innumerabiles numeri $aa+3bb$ exhiberi queant, qui omnes sint divisibiles per $pp+3qq$; eiusmodi nempe numeri obtinentur capiendo

$$a=3mq\pm np \quad \text{et} \quad b=mp\mp nq$$

neque hic amplius opus est conditionem adiecisse, ut $pp+3qq$ sit numerus primus, quoniam his valoribus assumtis in genere fit

$$aa+3bb=(pp+3qq)(nn+3mm).$$

COROLLARIUM 4

18. Hinc igitur vicissim intelligitur, si duo pluresve numeri quicunque formae $aa+3bb$ in se invicem multiplicentur, productum semper fore numerum eiusdem formae. Quod enim de producto duorum valet, facile ad productum quotcunque talium numerorum extenditur.

SCHOLION

19. Etiamsi autem verum sit productum ex duobus numeris formae $aa + 3bb$ itidem esse numerum eiusdem formae, tamen hinc per legitimam consequentiam nondum inferre licet, si numerus formae $aa + 3bb$ divisorem habeat quemcunque $pp + 3qq$, tum etiam quotum eiusdem formae esse futurum; tametsi enim et hoc verum sit, tamen peculiari indiget demonstratione mox exponenda. Eiusmodi autem conclusionem illicitam esse vel ex hoc exemplo patebit: Cum productum ex duobus numeris paribus sit numerus par, si quis inde concludere vellet numerum parem per parem divisum quotum etiam parem esse praebiturum, is certe falleretur.[1]) Demonstrationem ergo huius veritatis a divisore primo formae $pp + 3qq$ sum exorsus, quae conditio eatenus demonstrationem afficit, quod absque ea perperam concluderetur, cum productum $(aq + bp)(aq - bp)$ sit divisibile, alterutrum factorem divisibilem esse debere per $pp + 3qq$. Deinde vero etiam ex eo, quod p et q sint numeri inter se primi, derivavimus producti $p(mp \pm b)$, quod per q est divisibile, factorem $mp \pm b$ per q divisibilem esse debere; quae posterior conditio cum priore necessario est connexa.

PROPOSITIO 5

20. *Si numerus $aa + 3bb$ fuerit divisibilis per productum ex duobus pluribusve numeris primis formae $pp + 3qq$, tum etiam quotus erit numerus eiusdem formae, puta $nn + 3mm$.*

DEMONSTRATIO

Sint enim P, Q, R etc. numeri primi formae $pp + 3qq$ numerusque $aa + 3bb$ divisibilis per productum PQR. Sit M quotus inde resultans, ita ut sit $aa + 3bb = MPQR$. Cum igitur sit $\frac{aa + 3bb}{P} = MQR$, erit per propositionem praecedentem MQR numerus eiusdem formae. Ponatur itaque $MQR = cc + 3dd$; erit $\frac{cc + 3dd}{Q} = MR$ ideoque ob eandem rationem hic quotus MR numerus eiusdem formae; statuatur itaque $MR = ee + 3ff$, et cum sit $\frac{ee + 3ff}{R} = M$, erit pariter M numerus formae $nn + 3mm$.

1) Confer Commentationem 228 huius voluminis, § 6. F. R.

COROLLARIUM 1

21. Si ergo numerus $aa + 3bb$ fuerit productum ex numeris quotcunque primis P, Q, R, S etc. formae $pp + 3qq$ et praeterea numero M, ita ut sit $aa + 3bb = MPQRS$ etc., certo affirmare poterimus hunc numerum M esse eiusdem formae seu $M = nn + 3mm$.

COROLLARIUM 2

22. Quodsi igitur numerus $aa + 3bb$ unum habeat factorem A, qui non sit numerus formae $nn + 3mm$, tum alter factor neque erit numerus primus formae $pp + 3qq$ neque productum ex duobus pluribusve huiusmodi numeris primis.

COROLLARIUM 3

23. Eodem ergo casu si ponamus $aa + 3bb = AB$ et A non fuerit numerus formae $nn + 3mm$, tum B unum saltem factorem primum complectetur, qui non erit huius formae. Nam si B est numerus primus, non erit formae $pp + 3qq$; sin autem non est primus, quia non ex meris numeris primis formae $pp + 3qq$ constabit, unum ad minimum factorem continebit, qui non sit eiusdem formae.

COROLLARIUM 4

24. At si existente $aa + 3bb = AB$ factor A non fuerit numerus formae $nn + 3mm$, tum vel ipse erit numerus primus in hac forma non contentus vel saltem factorem implicabit primum in hac forma non contentum; si enim A ex meris numeris primis formae $pp + 3qq$ esset conflatus, ipse foret numerus eiusdem formae.

COROLLARIUM 5

25. Hinc sequitur, si numerus $aa + 3bb$ unum habeat factorem primum in forma $pp + 3qq$ non contentum, tum eum insuper certo adhuc alium factorem involvere, qui aeque non in hac forma $pp + 3qq$ contineatur.

COROLLARIUM 6

26. Ita iam ante vidimus, si numerus $aa + 3bb$ sit par seu factorem habeat 2, qui numerus non est formae $pp + 3qq$, tum eum insuper eundem factorem 2 complecti seu non solum per 2, sed etiam per 4 esse divisibilem.

SCHOLION

27. Exhiberi quidem possunt numeri formae $aa+3bb$, qui per numerum quemcunque N sint divisibiles, etiamsi N non sit numerus formae $pp+3qq$, dum scilicet pro a et b multipla quaecunque huius numeri N accipiuntur; ita posito $a=mN$ et $b=nN$ numerus $aa+3bb=NN(mm+3nn)$ non solum per N, sed adeo per eius quadratum NN fit divisibilis; hocque ergo casu utique duo adsunt factores N et N, quorum neuter in forma $pp+3qq$ continetur, uti § 25 ostendimus. Verum si a et b sint numeri inter se primi, hic casus locum habere nequit, ex quo merito dubitamus, num numerus inde formatus $aa+3bb$ praeter binarium ullum admittat divisorem, qui non sit formae $pp+3qq$. De binario quidem hoc negari nequit, cum, quoties a et b fuerint numeri impares ambo, divisio per 2 succedat; at vero tum insuper binarius inest, qui cum illo coniunctus praebet factorem 4 quasi simplicem spectandum. Diligentius igitur examinandum restat, utrum, dum a et b sunt primi inter se, numerus $aa+3bb$ habeat ullum divisorem primum, qui non in forma $pp+3qq$ contineatur, necne; quod quidem esse negandum mox rigide sum demonstraturus; in quo negotio autem probe est cavendum, ne casus binarii, quem excipi oportet, in demonstratione quicquam turbet.

PROPOSITIO 6

28. *Si daretur numerus primus A in forma $pp+3qq$ non contentus, qui esset divisor cuiuspiam numeri $aa+3bb$ numeris a et b existentibus inter se primis, tum exhiberi posset alius numerus primus praeter binarium minor B in forma $pp+3qq$ pariter non contentus, qui etiam futurus esset divisor cuiuspiam numeri formae $aa+3bb$, in quo numeri a et b itidem forent inter se primi.*

DEMONSTRATIO

Quia a et b sunt numeri primi inter se et $aa+3bb$ per A divisibilis ponitur, erunt ii quoque primi ad A. Si illi numeri essent maiores quam A, statui posset

$$a=mA\pm c \quad \text{et} \quad b=nA\pm d,$$

ut numeri c et d, qui pariter tam inter se[1]) quam ad A futuri essent primi, forent semissi ipsius A minores, scilicet $c < \frac{1}{2}A$ et $d < \frac{1}{2}A$, quia A utpote primus est impar; casum enim, quo $A = 2$, hinc excipimus. Prodiret autem hac positione

$$aa + 3bb = mmAA \pm 2mAc + cc + 3nnAA \pm 6nAd + 3dd$$

hincque obtineretur numerus $cc + 3dd$ minor quam AA, qui esset per A divisibilis, et quotus foret minor quam A. Cum igitur A sit per hypothesin numerus in forma $pp + 3qq$ non contentus, vel ipse quotus, si fuerit primus, non erit numerus formae $pp + 3qq$ vel, si sit compositus, factorem habebit primum in hac forma non contentum. Sit B vel ipse quotus vel iste eius factor eritque certe $B < A$, ex quo daretur numerus primus B minor quam A in forma $pp + 3qq$ non contentus, qui esset divisor numeri $cc + 3dd$ existentibus numeris c et d inter se primis.

Dico autem hunc numerum primum B a binario fore diversum. Vel enim quotus $\frac{cc+3dd}{A}$ foret impar vel par; et casu priori binarius in eo non contineretur sicque numerus B non esset 2. Casu autem posteriori quotus binarium quidem atque adeo quaternarium involveret; unde cum 4 sit numerus formae $pp + 3qq$, necesse esset, ut ille quotus alium insuper factorem primum in forma $pp + 3qq$ non contentum implicaret. Vel si $cc + 3dd$ esset per 4 divisibilis, quod eveniret, si uterque numerus c et d esset impar, eius quadrans $\frac{1}{4}(cc + 3dd)$ ad formam $ee + 3ff$ reduci posset; quae cum per A etiamnunc foret divisibilis, multo magis quotus $\frac{ee+3ff}{A}$ implicaret factorem primum imparem in forma $pp + 3qq$ non contentum.

PROPOSITIO 7

29. *Omnes numeri huius formae $aa + 3bb$, siquidem a et b sint numeri primi inter se, praeter binarium nullos admittunt divisores primos, nisi qui ipsi in forma $pp + 3qq$ contineantur.*

---

1) Numeros c et d inter se primos esse demonstrari non potest. Sed etiamsi communem divisorem haberent, tamen sequentia valerent. Si enim esset $c = ke$ et $d = kf$ existentibus e et f numeris inter se primis, ex divisibilitate formulae $c^2 + 3d^2 = k^2(e^2 + 3f^2)$ sequeretur formulam $e^2 + 3f^2$ per A esse divisibilem etc. F. R.

DEMONSTRATIO

Si enim numerus quispiam formae $aa + 3bb$ haberet factorem primum quantumvis magnum A, qui in forma $pp + 3qq$ non contineretur, ex eo inveniri posset alius numerus primus B minor quam A nec in forma $pp + 3qq$ contentus, qui pariter esset divisor cuiuspiam numeri formae $aa + 3bb$ existentibus a et b numeris inter se primis; atque ex hoc numero B simili modo alii C, D, E continuo minores eiusdem indolis inveniri possent haecque diminutio nunquam terminaretur neque etiam unquam ad binarium perveniretur. Cum igitur exhibitio numerorum integrorum continuo minorum involvat contradictionem, sequitur praeter binarium nullum dari numerum primum in forma $pp + 3qq$ non contentum, per quem ullus numerus formae $aa + 3bb$ dividi queat existentibus a et b numeris inter se primis.

COROLLARIUM 1

30. Omnes ergo divisores primi, qui conveniunt numeris formae $aa + 3bb$, siquidem a et b sint numeri inter se primi, ipsi in eadem forma $pp + 3qq$ continentur, dummodo hinc binarius excludatur.

COROLLARIUM 2

31. Si igitur numeri primi in duas classes distribuantur, quarum prior contineat eos, qui sunt formae $pp + 3qq$, posterior vero eos, qui ad hanc formam reduci nequeunt, omnes numeri huius posterioris classis ex serie divisorum numerorum formae $aa + 3bb$ excluduntur.

COROLLARIUM 3

32. Nisi ergo numerus $aa + 3bb$ existentibus a et b numeris inter se primis ipse sit primus, erit is productum ex meris numeris primis formae $pp + 3qq$, dummodo quaternarius etiam inter hos numeros referatur.

SCHOLION

33. Quod productum ex duobus pluribusve numeris formae $pp + 3qq$ iterum in forma $aa + 3bb$ contineatur, supra ostendimus; indeque ergo patebat, si P, Q, R, S etc. denotent numeros primos in forma $pp + 3qq$

contentos, productum ex quotcunque huiusmodi numeris P, Q, R, S etc. semper ad formam $aa+3bb$ revocari posse. Nunc autem huius propositionis inversam demonstravimus, qua patet numeros formae $aa+3bb$ nullos alios factores admittere, nisi qui ipsi sint numeri formae $pp+3qq$. Hic quidem assumsimus numeros a et b esse primos inter se; sin autem non essent primi, sed maximum haberent divisorem communem m, ut sit $a=mc$ et $b=md$, tum numerus $aa+3bb=mm(cc+3dd)$ primum habebit factorem quadratum mm, cuius radix potest esse numerus quicunque, praeterea vero alios non involvet factores primos, nisi qui ipsi sint formae $pp+3qq$.

PROPOSITIO 8

34. *Omnis numerus primus formae $pp+3qq$, si per 6 dividatur, relinquit unitatem seu in forma numerorum $6n+1$ continetur excepto ternario, qui etiam in forma $pp+3qq$ continetur.*

DEMONSTRATIO

Cum $pp+3qq$ sit numerus primus, quadratum pp per ternarium non est divisibile, sed per 3 divisum relinquit 1; quia ergo $3qq$ divisionem per 3 admittit, summa $pp+3qq$ per 3 divisa residuum dabit $=1$ eritque propterea numerus formae $3m+1$. Cum autem $pp+3qq$ simul sit numerus impar per hypothesin, necesse est, ut m sit numerus par; unde posito $m=2n$ formula $6n+1$ omnes complectetur numeros primos in forma $pp+3qq$ contentos, excepto scilicet ternario ipso, cuius singularis est ratio.

COROLLARIUM 1

35. Quia omnes numeri primi exceptis 2 et 3 vel in hac formula $6n+1$ vel in hac $6n-1$ continentur, evidens est nullos numeros primos posterioris formae $6n-1$ in forma $pp+3qq$ contineri.

COROLLARIUM 2

36. Hinc omnes numeri primi formae $6n-1$, qui sunt

5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89 etc.,

ex divisoribus numerorum formae $aa+3bb$ sunt excludendi seu nullus numerus huius formae $aa+3bb$, dum quidem sint a et b numeri primi inter se, exhiberi potest, qui per ullum numerum primum formae $6n-1$ sit divisibilis.

SCHOLION

37. Utrum autem omnes numeri primi alterius formae $6n+1$, qui sunt

$$7,\ 13,\ 19,\ 31,\ 37,\ 43,\ 61,\ 67,\ 73,\ 79,\ 97 \text{ etc.},$$

sint divisores numerorum formae $aa+3bb$ seu, quod eodem redit, an omnes in forma $pp+3qq$ contineantur, ex allatis nondum affirmare licet. Inde enim tantum constat omnes numeros primos formae $pp+3qq$ simul in forma $6n+1$ contineri et propositio inversa peculiari indiget demonstratione; quae ita concinnari debet, ut proposito numero primo formae $6n+1$ quocunque ostendatur semper quempiam numerum formae $aa+3bb$, in quo a et b sint numeri primi inter se, exhiberi posse, qui per illum numerum $6n+1$ sit divisibilis; in quo negotio loco formae $aa+3bb$ etiam haec $ff\pm fg+gg$ illi aequivalens accipi potest. Si enim numerorum f et g alteruter, puta g, fuerit par, erit

$$ff\pm fg+gg=\left(f\pm\tfrac{1}{2}g\right)^2+3\left(\tfrac{1}{2}g\right)^2;$$

sin autem uterque sit impar, erit tam $f+g$ quam $f-g$ numerus par et

$$ff\pm fg+gg=\left(\frac{f\mp g}{2}\right)^2+3\left(\frac{f\pm g}{2}\right)^2.\text{ [1]}$$

Quodsi ergo exhiberi queat numerus $ff\pm fg+gg$ per numerum primum $6n+1$ divisibilis, ita ut f et g sint primi inter se, simul constabit numerum $6n+1$ esse numerum in forma $pp+3qq$ contentum; id quod in sequente propositione demonstrabimus.

---

1) Editio princeps (atque etiam *Comment. arithm.*):

$$ff\pm fg+gg=\frac{(f\mp g)^2}{2}+3\,\frac{(f\pm g)^2}{2}.$$

Correxit F. R.

PROPOSITIO 9

38. *Omnis numerus primus formae* $6n+1$ *simul in hac forma* $pp+3qq$ *continetur.*

DEMONSTRATIO

Iam dudum demonstravi, si $6n+1$ fuerit numerus primus, per eum divisibiles esse omnes numeros in hac forma $a^{6n}-b^{6n}$ contentos, dummodo neuter numerorum a et b seorsim per $6n+1$ sit divisibilis.[1] Cum igitur in factores resolvendo sit

$$a^{6n}-b^{6n}=(a^{2n}-b^{2n})(a^{4n}+a^{2n}b^{2n}+b^{4n}),$$

alteruter horum factorum per $6n+1$ sit divisibilis necesse est. Quodsi ergo dentur casus, quibus factor $a^{2n}-b^{2n}$ non sit divisibilis per $6n+1$, ut tamen neque a neque b per eum sit divisibilis, iis casibus certe alter factor $a^{4n}+a^{2n}b^{2n}+b^{4n}$, hoc est numerus formae $ff+fg+gg$, per $6n+1$ erit divisibilis ideoque numerus primus $6n+1$ foret in forma $pp+3qq$ contentus. Demonstrari igitur debet dari casus, quibus forma $a^{2n}-b^{2n}$ non sit divisibilis per $6n+1$. Ad hoc efficiendum sumo $b=1$ et ostendam fieri non posse, ut omnes isti numeri

$$2^{2n}-1,\quad 3^{2n}-1,\quad 4^{2n}-1,\quad 5^{2n}-1,\ \ldots\ (6n)^{2n}-1$$

sint per $6n+1$ divisibiles, ubi quidem pro a omnes numeros ipso $6n+1$ minores ideoque primos ad eum assumi pono. Nam si omnes hi numeri per $6n+1$ essent divisibiles, eorum etiam differentiae cum primae tum secundae et sequentes omnes per $6n+1$ essent divisibiles ideoque etiam differentiae ordinis $2n$, quae sunt omnes constantes et hoc modo exprimuntur

$$2^{2n}-\frac{2n}{1}\cdot 3^{2n}+\frac{2n(2n-1)}{1\cdot 2}\cdot 4^{2n}-\frac{2n(2n-1)(2n-2)}{1\cdot 2\cdot 3}\cdot 5^{2n}+\cdots+(2+2n)^{2n},$$

ubi, cum sit $2n+2<6n$, nullae potestates numerorum per $6n+1$ divisibilium ingrediuntur. Aliunde autem constat differentiam ordinis $2n$ esse $=1\cdot 2\cdot 3\cdot 4\cdots 2n$; quae cum certe non sit per $6n+1$ divisibilis, manifesto indicat reperiri adeo inter hos numeros

$$2^{2n}-1,\quad 3^{2n}-1,\quad 4^{2n}-1,\ \ldots\ (2+2n)^{2n}-1$$

1) Vide Commentationem 134 huius voluminis, theorema 4. F. R.

unum vel etiam plures, qui non sint per $6n+1$ divisibiles. Dum autem unicus detur huiusmodi numerus $a^{2n}-1$ per $6n+1$ non divisibilis, per eum erit divisibilis $a^{4n}+a^{2n}+1$, hoc est numerus formae $ff+fg+gg$, in quo neque f neque g sit per $6n+1$ divisibilis. Consequenter numerus primus $6n+1$ est formae $pp+3qq$.[1])

SCHOLION

39. Omnia ergo, quae cum in demonstratione theorematis non dari duos cubos, quorum summa sit cubus[2]), tum in solutione problematis de inveniendis tribus cubis, quorum summa sit cubus, assumseram, iam plane rigide sunt demonstrata. Assumseram autem primo numeros formae $aa+3bb$ seu $ff\pm fg+gg$ nullos admittere divisores primos, nisi qui ipsi sint eiusdem formae, deinde omnes numeros primos istius formae simul in formula $6n+1$ contineri ac vicissim omnes numeros primos in formula $6n+1$ contentos simul esse numeros formae $pp+3qq$. Quare nunc tam illa demonstratio quam solutio pro perfectis sunt habendae.

Interim tamen fateri cogor in hac de natura numerorum Theoria plurima etiamnum desiderari atque FERMATII demonstrationes deperditas sine dubio multo profundiores speculationes in se esse complexas. Eo enim modo, quo usus sum ad demonstrandum summam duorum cuborum nunquam posse esse cubum, non perspicio, quomodo demonstratio ad potestates altiores extendi possit, cum tamen FERMATIUS demonstrationem habuerit neque summam a^n+b^n neque differentiam a^n-b^n nunquam esse potestatem similis exponentis c^n, quando exponens n fuerit binario maior.[3]) Demonstrandum ergo esset hanc aequationem $a^n\pm b^n=c^n$ in rationalibus nunquam locum habere posse, statim atque exponens n binarium superet, nisi unus numerorum a, b, c evanescat. Deinde, etsi demonstravi numeros primos omnes

1) Confer hanc demonstrationem, quae in consideratione differentiarum versatur, cum demonstrationibus eodem fundamento innitentibus, quas EULERUS in Commentationibus 241, § 5, et 262, § 72, exposuit. F. R.

2) Sed vide notam 1 p. 558. F. R.

3) Vide FERMATII observationem ad quaestionem VIII libri II DIOPHANTI *Arithmeticorum* (cf. notam 2 p. 51 et notam p. 404); *Oeuvres de Fermat*, t. I, p. 291. Celeberrima FERMATII observatio marginalis haec est:

„Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duas eiusdem nominis fas est dividere: cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet". F. R.

formae $6n+1$ esse in formula $pp+3qq$ contentos, tamen simili modo demonstrare non licet numeros primos formae $8n+3$ semper in forma $pp+2qq$ contineri, quod tamen aeque est certum et a FERMATIO demonstratum.[1]) Successit mihi quidem demonstratio, quod numeri primi formae $4n+1$ sint omnes duorum quadratorum summae[2]), similique modo demonstrare possum omnes numeros primos formae $8n+1$ simul in forma $pp+2qq$ contineri; verum plurima eiusdem generis theoremata proferri possunt aeque vera, veluti quod omnes numeri primi vel huius formae $20n+1$ vel $20n+9$ simul in formula $pp+5qq$ contineantur[3]), et huiusmodi plura alia, quae tamen nondum video, quomodo demonstrari queant. Ex quo Theoria numerorum nobis adhuc maximam partem abscondita est censenda.

---

1) Vide Commentationem 256 huius voluminis, imprimis § 56 atque notam 1 p. 485. F. R.

2) Vide Commentationem 241 huius voluminis. F. R.

3) Vide huius voluminis Commentationem 164, theoremata 10—12, imprimis notam p. 194. F. R.

DE RESOLUTIONE FORMULARUM QUADRATICARUM INDETERMINATARUM PER NUMEROS INTEGROS[1]

Commentatio 279 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 9 (1762/3), 1764, p. 3—39
Summarium ibidem p. 5—8

SUMMARIUM[2]

Consideratio numerorum, quamvis plerisque omni usu carere videatur, tamen per se non solum admodum est iucunda, sed etiam animum ad veritatis indagationem non mediocriter acuit eiusque vires quasi magis intendit. Maxime enim abundat doctrina numerorum veritatibus abstrusissimis, quarum investigatio et demonstratio tantam ingenii penetrationem postulat, ut nunquam cuncta, quae involvit, mysteria erui et explicari posse videantur. Quod certe eo magis mirum videri debet, quod numeri nusquam per se revera existant, sed per solam abstractionem in mente formentur, qua primo quidem series numerorum naturalium ab unitate in infinitum progredientium constituitur, tum vero ad intervalla implenda numeri fracti et surdi atque adeo transcendentes introducuntur. Quorum generum tractatio etsi ad Arithmeticam referri solet, tamen in hac scientia insignes proprietates, quibus numeri sunt affecti, vix attinguntur, quippe quae vulgo tantum ad usitatas numerorum operationes explicandas restringitur.

Accuratius autem numerorum natura investigatur in ea Analyseos parte, quae ab antiquissimo Auctore methodus DIOPHANTEA vocari solet, ubi eiusmodi problemata perpenduntur, quae in se sunt indeterminata atque infinitas solutiones admittunt, ex quibus autem

---

1) Confer cum hac dissertatione Commentationem 29 huius voluminis. F. R.

2) Nonnulli errores, qui in editione principe huius Summarii inveniuntur, secundum manuscriptum correcti sunt. F. R.

eas elici oportet, quae numeris vel saltem rationalibus vel integris tantum contineantur. Cuius methodi vis per exemplum clarissime perspicietur. Sumamus igitur eiusmodi numeros quaeri debere, quorum quadrata duplicata unitate aucta iterum fiant quadrata, seu ut forma $2xx+1$ extractionem radicis quadratae admittat. Quodsi fractiones non excludantur, huic quaestioni facillime satisfit aequando formulam $2xx+1$ huic quadrato $(xy-1)^2$. Quia enim aequatio $2xx+1=xxyy-2xy+1$ unitate utrinque deleta per x divisionem admittit, prodit $2x=xyy-2y$ hincque

$$x=\frac{2y}{yy-2},$$

ubi, quicunque numeri pro y accipiantur sive integri sive fracti, pro x semper eiusmodi numeri rationales resultant, quibus formula $2xx+1$ evadit quadratum, quippe cuius radix quadrata futura est $xy-1$. Qui numeri quo facilius obtineantur, loco y scribi potest fractio $\pm\frac{p}{q}$, unde prodit vel $x=\frac{2pq}{pp-2qq}$ vel $x=\frac{2pq}{2qq-pp}$. Hic igitur sufficit pro p et q numeros quoscunque integros accipi; veluti si capiatur $p=5$ et $q=3$, prodit $x=\frac{30}{7}$, qui est huiusmodi numerus, ut eius quadratum $\frac{900}{49}$ si duplicetur $\frac{1800}{49}$ et unitas adiiciatur $\frac{1849}{49}$, summa haec sit quadratum radice existente $\frac{43}{7}$. Verum si pro x tantum numeri integri desiderentur, qui hac proprietate gaudeant, solutio modo data nihil utilitatis affert, cum pro p et q eiusmodi numeri assumi deberent, ut $2pq$ divisibile fieret per $pp-2qq$, quod non minus est difficile quam ipsum problema, de quo agitur. Interim tamen hac conditione adiecta problema etiamnum recipit innumeras solutiones et numeri pro x assumendi hac lege procedunt

$$0,\ 2,\ 12,\ 70,\ 408,\ 2378,\ 13860 \text{ etc.},$$

ubi continuo sequens aequatur sextuplo ultimi demto penultimo, cuiusmodi series vocari solent recurrentes, unde evidens est et harum solutionum multitudinem esse infinitam, etiamsi continuo rarius occurrant. Ideoque facile intelligitur earum inventionem multo magis esse arduam.

Cel. Auctor huius dissertationis methodum peculiarem exponit huiusmodi problemata facile resolvendi, quibus in genere omnes numeri integri pro x assumendi quaeruntur, ut haec formula $\alpha xx+\beta x+\gamma$ evadat numerus quadratus, dum α, β, γ denotant numeros quoscunque datos. Ubi primo quidem observat solutionem non succedere, nisi α sit numerus positivus non quadratus, tum vero necesse esse, ut una saltem solutio iam aliunde sit cognita; cuiusmodi solutio unica statim ac si praesto fuerit, quemadmodum inde omnes reliquae in infinitum inveniri queant, perspicue docet. Cum autem hoc problema iam alibi[1]) sit pertractatum, etsi methodo minus commoda, Auctor hic imprimis naturam huius-

1) Scilicet in Commentatione 29 huius voluminis. F. R.

modi problematum accuratius perscrutatur et criteria elicit, quibus problemata huius generis impossibilia a possibilibus distingui possunt. Denotante scilicet α numerum quemcunque positivum non quadratum, quia expressionem superiorem semper ad hanc formam $\alpha xx + \gamma$ revocare licet, ostendit, quinam numeri pro γ assumti problema reddant possibile necne. Veluti si sit $\alpha = 3$, notum est has formulas $3xx + 2$, $3xx + 5$, $3xx + 8$ etc. nunquam fieri posse quadratas. In maioribus autem numeris pro α sumtis hoc iudicium multo magis fit arduum; verumtamen Auctor criteria certissima indicat, quibus in omnibus casibus expedite uti licet, ubi multa, quibus miranda numerorum natura non mediocriter illustratur, occurrunt, et quae in aliis quaestionibus usum insignem habitura videntur.

PROBLEMA 1

1. *Proposita formula irrationali*

$$\sqrt{(\alpha xx + \beta x + \gamma)}$$

invenire numeros pro x substituendos, qui eam rationalem reddant.

SOLUTIO

Ante omnia notandum est hanc investigationem frustra suscipi, nisi unus saltem casus constet, quo ea fiat rationalis. Ponamus ergo hoc evenire casu $x = a$ eoque esse

$$\sqrt{(\alpha aa + \beta a + \gamma)} = b,$$

ita ut b sit numerus rationalis. Huiusmodi autem casus unico cognito innumerabiles alios ex eo derivare licet. Ponatur in hunc finem

$$x = a + mz \quad \text{et} \quad \sqrt{(\alpha xx + \beta x + \gamma)} = b + nz$$

et hac aequatione quadrata fit

$$\begin{aligned} &+ \alpha aa + 2\alpha maz + \alpha mmzz = bb + 2nbz + nnzz. \\ &+ \beta a + \quad \beta mz \\ &+ \gamma \end{aligned}$$

Cum iam per hypothesin sit $bb = \alpha aa + \beta a + \gamma$, reliqua aequatio per z

divisa dabit

$$2\alpha ma + \beta m + \alpha mmz = 2nb + nnz,$$

ex qua elicitur

$$z = \frac{2\alpha ma - 2nb + \beta m}{nn - \alpha mm}.$$

Quo valore substituto concludimus, si ponatur

$$x = \frac{(nn + \alpha mm)a - 2mnb + \beta mm}{nn - \alpha mm},$$

fore

$$\sqrt{(\alpha xx + \beta x + \gamma)} = \frac{2\alpha mna - (nn + \alpha mm)b + \beta mn}{nn - \alpha mm}.$$

Quicunque ergo numeri pro m et n accipiantur, ex casu cognito

$$\sqrt{(\alpha aa + \beta a + \gamma)} = b$$

infinitis aliis modis formula $\sqrt{(\alpha xx + \beta x + \gamma)}$ rationalis effici potest, et quia numerum b tam negative quam affirmative assumere licet, exploratis numeris a et b ac pro lubitu assumtis numeris m et n capiatur

$$x = \frac{(nn + \alpha mm)a \pm 2mnb + \beta mm}{nn - \alpha mm}$$

eritque

$$\sqrt{(\alpha xx + \beta x + \gamma)} = \frac{2\alpha mna \pm (nn + \alpha mm)b + \beta mn}{nn - \alpha mm}.$$

SCHOLION

2. Ad hoc ergo problema solvendum necesse est, ut aliunde unus saltem casus sit cognitus, quo formula proposita fiat rationalis. Neque vero pro huiusmodi casu explorando ulla certa regula praescribi potest, cum etiam dentur eiusmodi formulae, quas nullo plane casu rationales fieri posse demonstratum est. Si enim verbi gratia haec formula $\sqrt{(3xx + 2)}$ proponeretur, certum est nullum numerum rationalem pro x inveniri posse, quo ea fieret rationalis. Quanquam autem satis noti sunt casus, quibus formula $\alpha xx + \beta x + \gamma$ talis reductionis est capax, quippe quod evenit, quoties in hac formula generali $(px + q)^2 + (rx + s)(tx + u)$ continetur, tamen hic non curo, unde casus ille, quem cognitum assumo, sit haustus, sive certa quadam ratione sive divinatione innotuerit. Verum cum cognito uno casu inventio infini-

torum aliorum nulla laboret difficultate, hic potissimum ad solutiones, quae numeris integris absolvuntur, respicio. Cum enim valores pro x inventi per fractionem exprimantur, nova iam oritur quaestio, quomodo numeros m et n assumi oporteat, ut inde numeri integri pro x obtineantur.

PROBLEMA 2

3. *Si α, β, γ sint numeri integri dati, invenire numeros integros pro x sumendos, qui formulam $\alpha xx+\beta x+\gamma$ quadratam reddant.*

SOLUTIO

Iterum assumo unum numerum integrum a constare, qui quaesito satisfaciat, ita ut sit

$$\sqrt{(\alpha aa+\beta a+\gamma)}=b,$$

ac modo vidimus, si sumatur

$$x=\frac{(nn+\alpha mm)a\pm 2mnb+\beta mm}{nn-\alpha mm},$$

fore

$$\sqrt{(\alpha xx+\beta x+\gamma)}=\frac{2\alpha mna\pm(nn+\alpha mm)b+\beta mn}{nn-\alpha mm}.$$

Superest ergo tantum, ut videamus, cuiusmodi numeros pro m et n assumi oporteat, ut hae formulae integrae evadant. Quod quidem statim fieri perspicuum est, si utriusque denominator $nn-\alpha mm$ statuatur unitati aequalis. Sit igitur

$$nn-\alpha mm=1 \quad \text{seu} \quad nn=\alpha mm+1\,[1])$$

ideoque

$$n=\sqrt{(\alpha mm+1)};$$

nisi autem sit α vel numerus quadratus vel negativus, huic formulae semper satisfieri potest; sin autem sit vel quadratus vel negativus, ne problema quidem propositum resolvere licet. Etsi enim quandoque duo pluresve casus assignari queant, tamen infiniti non dantur, cuiusmodi tamen hic evolvi con-

1) De hac aequatione FERMATIANA vide notas p. 11 et 12. F. R.

venit. Sit ergo α numerus integer positivus non quadratus ac semper numeri m et n assignari possunt, ut fiat $n = V(\alpha mm + 1)$; quod etsi infinitis modis fieri potest, tamen sufficit minimos solos nosse. Erit ergo

$$x = (nn + \alpha mm)a \pm 2mnb + \beta mm$$

et

$$V(\alpha xx + \beta x + \gamma) = 2\alpha mna \pm (nn + \alpha mm)b + \beta mn$$

sicque habetur novus casus quaestioni satisfaciens. Ex hoc vero simili modo, quo is ex a et b prodiit, novus derivabitur hincque porro continuo alii in infinitum. Ponantur enim valores hoc modo pro x oriundi successive

$$a, \quad a^{\mathrm{I}}, \quad a^{\mathrm{II}}, \quad a^{\mathrm{III}} \quad \text{etc.},$$

respondentes vero valores formulae $V(\alpha xx + \beta x + \gamma)$ sint

$$b, \quad b^{\mathrm{I}}, \quad b^{\mathrm{II}}, \quad b^{\mathrm{III}} \quad \text{etc.}$$

ac sequenti modo bini quique posteriores ex binis antecedentibus definientur:

$$a^{\mathrm{I}} = (nn + \alpha mm)a \pm 2mnb + \beta mm, \quad b^{\mathrm{I}} = 2\alpha mna \pm (nn + \alpha mm)b + \beta mn,$$
$$a^{\mathrm{II}} = (nn + \alpha mm)a^{\mathrm{I}} \pm 2mnb^{\mathrm{I}} + \beta mm, \quad b^{\mathrm{II}} = 2\alpha mna^{\mathrm{I}} \pm (nn + \alpha mm)b^{\mathrm{I}} + \beta mn,$$
$$a^{\mathrm{III}} = (nn + \alpha mm)a^{\mathrm{II}} \pm 2mnb^{\mathrm{II}} + \beta mm, \quad b^{\mathrm{III}} = 2\alpha mna^{\mathrm{II}} \pm (nn + \alpha mm)b^{\mathrm{II}} + \beta mn$$

etc.

Hac igitur ratione continuo ulterius progredi licet sicque ex una solutione in numeris integris cognita innumerabiles aliae in numeris integris quoque elicientur.

COROLLARIUM 1

4. Ut igitur formula $\alpha xx + \beta x + \gamma$ infinitis modis in numeris integris quadratum effici possit, necesse est, ut α neque sit numerus quadratus neque negativus, ac praeterea, ut unus casus, quo ea fit quadratum, undecunque sit cognitus.

COROLLARIUM 2

5. At si α fuerit numerus positivus non quadratus, tum primum quaerantur duo numeri m et n, ut sit $n = V(\alpha mm + 1)$, id quod semper fieri

potest[1]). Quibus inventis si ponatur

$$\sqrt{(\alpha xx + \beta x + \gamma)} = y$$

atque iam cognitus fuerit casus quaestioni satisfaciens, qui sit $x = a$ et $y = b$, ex eo per primam operationem non solum unus, sed duo novi invenientur ob signi ambiguitatem. Erit quippe

$$x = (nn + \alpha mm)a \pm 2mnb + \beta mm$$

et

$$y = 2\alpha mna \pm (nn + \alpha mm)b + \beta mn.$$

COROLLARIUM 3

6. Si sumantur tantum signorum ambiguorum superiora, ut continuo ad maiores numeros satisfacientes perveniamus, atque valores pro x hoc modo successive prodeuntes designentur per a, a^{I}, a^{II}, a^{III}, a^{IV} etc., valores autem pro y respondentes per b, b^{I}, b^{II}, b^{III}, b^{IV} etc., erit

$$a^{\mathrm{I}} = (nn + \alpha mm)a + 2mnb + \beta mm, \quad b^{\mathrm{I}} = 2\alpha mna + (nn + \alpha mm)b + \beta mn,$$
$$a^{\mathrm{II}} = (nn + \alpha mm)a^{\mathrm{I}} + 2mnb^{\mathrm{I}} + \beta mm, \quad b^{\mathrm{II}} = 2\alpha mna^{\mathrm{I}} + (nn + \alpha mm)b^{\mathrm{I}} + \beta mn,$$
$$a^{\mathrm{III}} = (nn + \alpha mm)a^{\mathrm{II}} + 2mnb^{\mathrm{II}} + \beta mm, \quad b^{\mathrm{III}} = 2\alpha mna^{\mathrm{II}} + (nn + \alpha mm)b^{\mathrm{II}} + \beta mn$$

etc.

COROLLARIUM 4

7. Duplicem ergo hinc progressionem numerorum a, a^{I}, a^{II}, a^{III}, a^{IV} etc. et b, b^{I}, b^{II}, b^{III}, b^{IV} etc. adipiscimur, quarum utriusque continuatio ab utraque pendet, utraque tamen ab altera ita seiungi potest, ut termini utriusque sensim sine adminiculo alterius continuari queant; formabitur autem tum in utraque serie quilibet terminus ex binis praecedentibus.

COROLLARIUM 5

8. Si enim in valore a^{II} pro b^{I} eius valor substituatur, habebitur

$$a^{\mathrm{II}} = (nn + \alpha mm)a^{\mathrm{I}} + 4\alpha mmnna + 2mn(nn + \alpha mm)b + 2\beta mmnn + \beta mm.$$

1) Vide Commentationem 29 huius voluminis, § 16 et 17. F. R.

Verum ex valore ipsius a^{I} est $2mnb = a^{\text{I}} - (nn + \alpha mm)a - \beta mm$, quo valore ipsius $2mnb$ ibi substituto prodibit

$$a^{\text{II}} = (nn + \alpha mm)a^{\text{I}} + 4\alpha mmnna + (nn + \alpha mm)a^{\text{I}} - (nn + \alpha mm)^2 a - \beta mm(nn + \alpha mm) + 2\beta mmnn + \beta mm.$$

At ob $nn = \alpha mm + 1$ est

$$4\alpha mmnn - (nn + \alpha mm)^2 = -(nn - \alpha mm)^2 = -1$$

et

$$2\beta mmnn - \beta mm(nn + \alpha mm) = \beta mm(nn - \alpha mm) = \beta mm,$$

unde fit

$$a^{\text{II}} = 2(nn + \alpha mm)a^{\text{I}} - a + 2\beta mm.$$

COROLLARIUM 6

9. Cum igitur simili modo sit

$$a^{\text{III}} = 2(nn + \alpha mm)a^{\text{II}} - a^{\text{I}} + 2\beta mm \quad \text{etc.},$$

statim atque in serie a, a^{I}, a^{II}, a^{III} etc. duo primi termini habentur, primus scilicet a undecunque et secundus ex formula $a^{\text{I}} = (nn + \alpha mm)a + 2mnb + \beta mm$, ex his sequentes omnes per has formulas definientur

$$a^{\text{II}} = 2(nn + \alpha mm)a^{\text{I}} - a + 2\beta mm,$$
$$a^{\text{III}} = 2(nn + \alpha mm)a^{\text{II}} - a^{\text{I}} + 2\beta mm,$$
$$a^{\text{IV}} = 2(nn + \alpha mm)a^{\text{III}} - a^{\text{II}} + 2\beta mm$$
$$\text{etc.}$$

COROLLARIUM 7

10. Pari autem modo progressio numerorum b, b^{I}, b^{II}, b^{III} etc. est comparata. Primo enim eius termino aliunde cognito et secundo per formulam $b^{\text{I}} = 2\alpha mna + (nn + \alpha mm)b + \beta mn$, si in b^{II} pro a^{I} valor substituatur, erit

$$b^{\text{II}} = 2\alpha mn(nn + \alpha mm)a + 4\alpha mmnnb + 2\alpha\beta m^3 n + (nn + \alpha mm)b^{\text{I}} + \beta mn;$$

at ex valore ipsius b' est $2\alpha mna = b' - (nn + \alpha mm)b - \beta mn$, quo substituto fit ob $nn - \alpha mm = 1$

$$b'' = 2(nn + \alpha mm)b' - b$$

similiterque

$$b''' = 2(nn + \alpha mm)b'' - b',$$

$$b^{\text{IV}} = 2(nn + \alpha mm)b''' - b''$$

etc.

COROLLARIUM 8

11. Cum igitur utraque series ita sit comparata, ut quilibet terminus ex binis praecedentibus secundum certam legem definiatur, utraque series erit recurrens scala relationis existente $2(nn + \alpha mm), -1$. Hinc ergo formata aequatione

$$zz = 2(nn + \alpha mm)z - 1$$

eius radices erunt

$$z = 2nn - 1 \pm 2n\sqrt{(nn-1)} = (n \pm m\sqrt{\alpha})^2.$$

COROLLARIUM 9

12. Hinc ergo ex doctrina serierum recurrentium[1]) progressionis $a, a', a'', a''', a^{\text{IV}}$ etc. terminus quicunque indefinite per sequentem formulam[2]) exprimetur

$$\left(\frac{a}{2} + \frac{\beta}{4\alpha} + \frac{b}{2\sqrt{\alpha}}\right)(n + m\sqrt{\alpha})^{2\nu} + \left(\frac{a}{2} + \frac{\beta}{4\alpha} - \frac{b}{2\sqrt{\alpha}}\right)(n - m\sqrt{\alpha})^{2\nu} - \frac{\beta}{2\alpha} = x,$$

1) Vide L. EULERI *Introductionem in analysin infinitorum*, t. I cap. XIII, Lausannae 1748; *LEONHARDI EULERI Opera omnia*, series I, vol. 8. Vide praeterea EULERI Commentationem 453 (indicis ENESTROEMIANI): *Insignes proprietates serierum sub hoc termino generali contentarum*

$$x = \frac{1}{2}\left(a + \frac{b}{\sqrt{k}}\right)\left(p + q\sqrt{k}\right)^n + \frac{1}{2}\left(a - \frac{b}{\sqrt{k}}\right)\left(p - q\sqrt{k}\right)^n,$$

Novi comment. acad. sc. Petrop. 18 (1773), 1774, p. 198; *LEONHARDI EULERI Opera omnia*, series I, vol. 15. F. R.

2) Quae formula invenitur ope huius aequationis

$$P + Qz + 2\beta m^2 z^2(1 + z + z^2 + z^3 + \cdots) = (1 - 2(n^2 + \alpha m^2)z + z^2)(a + a^{\text{I}}z + a^{\text{II}}z^2 + a^{\text{III}}z^3 + \cdots)$$

existente $P = a$ et $Q = -a(n^2 + \alpha m^2) + 2mnb + \beta m^2$. Valor ipsius x oritur ex resolutione expressionis $\frac{P + Qz}{1 - 2(n^2 + \alpha m^2)z + z^2} + \frac{2\beta m^2 z^2}{(1-z)(1 - 2(n^2 + \alpha m^2)z + z^2)}$ in fractiones partiales. F. R.

alterius vero seriei b, b^{I}, b^{II}, b^{III} etc. terminus quicunque per hanc

$$\left(\frac{b}{2}+\frac{a\sqrt{\alpha}}{2}+\frac{\beta}{4\sqrt{\alpha}}\right)(n+m\sqrt{\alpha})^{2\nu}+\left(\frac{b}{2}-\frac{a\sqrt{\alpha}}{2}-\frac{\beta}{4\sqrt{\alpha}}\right)(n-m\sqrt{\alpha})^{2\nu}=y$$

sumto pro ν numero quocunque integro.

SCHOLION

13. Si hic pro 2ν substituamus successive omnes numeros integros 0, 1, 2, 3, 4, 5 etc., utraque progressio prodibit interpolata, cuius termini medii quaesito aeque satisfacient, dummodo fuerint integri. At reperiemus posito

$$2\nu=0\quad\begin{cases}x=a,\\ y=b,\end{cases}$$

$$2\nu=1\quad\begin{cases}x=na+mb+\dfrac{\beta}{2\alpha}(n-1),\\ y=nb+\alpha ma+\dfrac{1}{2}\beta m,\end{cases}$$

$$2\nu=2\quad\begin{cases}x=(nn+\alpha mm)a+2mnb+\beta mm,\\ y=(nn+\alpha mm)b+2\alpha mna+\beta mn.\end{cases}$$

Quae utraque series est recurrens scalam relationis habens $2n$, -1; ac pro priori quidem valorum ipsius x, si terni termini consecutivi sint P, Q, R, erit

$$R=2nQ-P+\frac{\beta(n-1)}{\alpha};\,^{1)}$$

at si in progressione valorum ipsius y terni termini se ordine sequentes sint P, Q et R, erit

$$R=2n\,Q-P.^{1)}$$

Quodsi ergo fuerit $\frac{\beta}{2\alpha}(n-1)$ numerus integer, omnes hi termini problema aeque resolvent sicque duplo plures obtinebimus solutiones, quam methodus adhibita suppeditaverat. Quod autem plures locum habere possint solutiones,

1) Haec progressionis lex congruit cum ea, quae etiam in huius voluminis Commentatione 29, § 7, exposita est. F. R.

quam invenimus, inde facile colligitur, quod praeter necessitatem primam erutarum formularum $nn - \alpha mm$ unitati aequalem posuimus, cum tamen sine dubio saepe etiam numerator per denominatorem dividi possit, etiamsi hic unitate sit maior. Quemadmodum igitur omnes plane solutiones in numeris integris inveniri queant, sequenti problemate accuratius examinemus.

PROBLEMA 3

14. *Si α sit numerus integer positivus non quadratus, dato uno numero integro a, qui pro x positus reddat formulam $\alpha xx + \beta x + \gamma$ quadratam, invenire infinitos alios numeros integros, qui pro x sumti idem sint praestituri.*

SOLUTIO

Ponatur in genere $\sqrt{(\alpha xx + \beta x + \gamma)} = y$, casu autem cognito, quo $x = a$, esse $\sqrt{(\alpha aa + \beta a + \gamma)} = b$ atque hinc in genere fractionibus non exclusis fore vidimus

$$x = \frac{(nn + \alpha mm)a + 2mnb + \beta mm}{nn - \alpha mm},$$

$$y = \frac{(nn + \alpha mm)b + 2\alpha mna + \beta mn}{nn - \alpha mm}.$$

Iam quidem, ut hi numeri fiant integri, non absolute necesse est, ut denominator $nn - \alpha mm$ ad unitatem revocetur, verum sufficit, ut fractiones $\frac{nn + \alpha mm}{nn - \alpha mm}$ et $\frac{2mn}{nn - \alpha mm}$ in numeros integros abeant. Ponamus ergo esse

$$\frac{nn + \alpha mm}{nn - \alpha mm} = p \quad \text{et} \quad \frac{2mn}{nn - \alpha mm} = q,$$

unde fit $p - 1 = \frac{2\alpha mm}{nn - \alpha mm}$ ideoque

$$\frac{\beta mm}{nn - \alpha mm} = \frac{\beta}{2\alpha}(p - 1) \quad \text{et} \quad \frac{\beta mn}{nn - \alpha mm} = \frac{1}{2}\beta q.$$

Deinde autem ex formulis assumtis fiet

$$pp - \alpha qq = \frac{(nn + \alpha mm)^2 - 4\alpha m^2 n^2}{(nn - \alpha mm)^2} = 1,$$

ita ut sit

$$pp = \alpha qq + 1 \quad \text{et} \quad p = \sqrt{(\alpha qq + 1)}.$$

Iterum igitur ut ante ex numero α binos numeros p et q assignari oportet, ut sit $p = \sqrt{(\alpha qq + 1)}$; quibus inventis habebitur

$$x = pa + qb + \frac{\beta}{2\alpha}(p - 1) \quad \text{et} \quad y = pb + \alpha qa + \frac{1}{2}\beta q.$$

Dummodo ergo fuerit $\frac{\beta}{2\alpha}(p - 1)$ numerus integer, hi valores satisfaciunt. Quia autem numeros p et q tam negative quam positive sumere licet, hae formulae insuper tres alias solutiones suppeditant

$$x = \quad pa - qb + \frac{\beta}{2\alpha}(p - 1) \quad \text{et} \quad y = \quad pb - \alpha qa - \frac{1}{2}\beta q,$$

$$x = -pa + qb - \frac{\beta}{2\alpha}(p + 1) \quad \text{et} \quad y = -pb + \alpha qa + \frac{1}{2}\beta q,$$

$$x = -pa - qb - \frac{\beta}{2\alpha}(p + 1) \quad \text{et} \quad y = -pb - \alpha qa - \frac{1}{2}\beta q.$$

Quodsi porro horum bini quicunque pro a et b assumantur, ex quolibet quatuor novae solutiones orientur. Hinc tamen non 16, sed tantum sex diversae oriuntur, inter quas adeo prima cognita $x = a$ et $y = b$ et, quae huic est affinis, $x = -a - \frac{\beta}{\alpha}$ et $y = -b$ continentur; reliquae vero quatuor sunt

$$x = \quad (pp + \alpha qq)a \pm 2pqb + \beta qq, \quad y = (pp + \alpha qq)b \pm 2\alpha pqa \pm \beta pq,$$

$$x = -(pp + \alpha qq)a \pm 2pqb - \frac{\beta}{\alpha}pp, \quad y = (pp + \alpha qq)b \mp 2\alpha pqa \mp \beta pq,$$

ex quibus deinceps novae aliae in infinitum inveniri possunt.

COROLLARIUM 1

15. Quodsi ergo fuerit vel $\beta = 0$ vel eiusmodi numerus, ut $\beta(p - 1)$ vel etiam $\beta(p + 1)$ per 2α divisibile existat, tum hoc modo plures solutiones in integris obtinentur quam modo ante exposito.

COROLLARIUM 2

16. In genere autem observandum est, si satisfecerit casus quicunque $x = v$, tum etiam satisfacturum esse casum $x = -v - \frac{\beta}{\alpha}$; ex utroque enim y eundem valorem nanciscitur. Quare cum hi casus ex illis tam facile eliciantur, his omissis investigatio solutionum convenientium ad dimidium reducitur.

COROLLARIUM 3

17. Reiectis ergo casibus $x = -v - \frac{\beta}{\alpha}$, quippe qui sponte se produnt inventis casibus $x = v$, ex casu $x = a$ et $y = b$ statim bini reperiuntur

$$x = pa \pm qb + \frac{\beta}{2\alpha}(p-1), \quad y = \alpha qa \pm pb + \frac{1}{2}\beta q$$

hincque porro per operationem secundam bini

$$x = (pp + \alpha qq)a \pm 2pqb + \beta qq, \quad y = 2\alpha pqa \pm (pp + \alpha qq)b + \beta pq,$$

quae duplicitas ex signo ambiguo numeri b nascitur.

COROLLARIUM 4

18. Si haec cum § 12 et 13 conferantur, patebit omnes has formulas in sequentibus expressionibus generalibus contineri, siquidem pro μ successive omnes numeri integri substituantur:

$$\text{I.}\begin{cases} x = \frac{1}{4\alpha}(2\alpha a + \beta + 2b\sqrt{\alpha})(p + q\sqrt{\alpha})^\mu + \frac{1}{4\alpha}(2\alpha a + \beta - 2b\sqrt{\alpha})(p - q\sqrt{\alpha})^\mu - \frac{\beta}{2\alpha}, \\ y = \frac{1}{4\sqrt{\alpha}}(2\alpha a + \beta + 2b\sqrt{\alpha})(p + q\sqrt{\alpha})^\mu - \frac{1}{4\sqrt{\alpha}}(2\alpha a + \beta - 2b\sqrt{\alpha})(p - q\sqrt{\alpha})^\mu \end{cases}$$

et

$$\text{II.}\begin{cases} x = \frac{1}{4\alpha}(2\alpha a + \beta - 2b\sqrt{\alpha})(p + q\sqrt{\alpha})^\mu + \frac{1}{4\alpha}(2\alpha a + \beta + 2b\sqrt{\alpha})(p - q\sqrt{\alpha})^\mu - \frac{\beta}{2\alpha}, \\ y = \frac{1}{4\sqrt{\alpha}}(2\alpha a + \beta - 2b\sqrt{\alpha})(p + q\sqrt{\alpha})^\mu - \frac{1}{4\sqrt{\alpha}}(2\alpha a + \beta + 2b\sqrt{\alpha})(p - q\sqrt{\alpha})^\mu. \end{cases}$$

COROLLARIUM 5

19. Hinc igitur duplices series pro valoribus numerorum x et y reperiuntur, quae eandem progressionis legem tenebunt. Si enim ponamus

$$x = a,\ a^{\text{I}},\ a^{\text{II}},\ a^{\text{III}},\ a^{\text{IV}},\ a^{\text{V}} \text{ etc.},\ P,\ Q,\ R,$$
$$y = b,\ b^{\text{I}},\ b^{\text{II}},\ b^{\text{III}},\ b^{\text{IV}},\ b^{\text{V}} \text{ etc.},\ S,\ T,\ V,$$

erit pro altera

$$a^{\text{I}} = pa + qb + \frac{\beta}{2\alpha}(p-1) \quad \text{et} \quad b^{\text{I}} = \alpha qa + pb + \frac{1}{2}\beta q$$

et pro altera

$$a^{\text{I}} = pa - qb + \frac{\beta}{2\alpha}(p-1) \quad \text{et} \quad b^{\text{I}} = \alpha qa - pb + \frac{1}{2}\beta q,$$

pro utraque vero haec communis progressionis lex valebit, ut sit

$$R = 2pQ - P + \frac{\beta}{\alpha}(p-1) \quad \text{et} \quad V = 2pT - S.$$

COROLLARIUM 6

20. Cum sit $pp - \alpha qq = 1$, erit

$$(p + q\sqrt{\alpha})^{\mu} = (p - q\sqrt{\alpha})^{-\mu} \quad \text{et} \quad (p - q\sqrt{\alpha})^{\mu} = (p + q\sqrt{\alpha})^{-\mu}$$

hincque, si alterae series retrorsum continuentur, prodibunt alterae. Sufficit ergo pro altero casu has series instruxisse, quae tam antrorsum quam retrorsum continuatae omnes solutiones ex ambiguitate numeri b oriundas in se continebunt.

SCHOLION

21. Si ergo fuerit $\beta = 0$, ut habeatur haec formula $\sqrt{(\alpha xx + \gamma)} = y$ rationalis reddenda, casusque constet, quo sit $\sqrt{(\alpha aa + \gamma)} = b$, sumtis numeris p et q ita, ut sit $p = \sqrt{(\alpha qq + 1)}$, innumerabiles alii valores satisfacientes continebuntur in his seriebus

$$x = a,\ a^{\text{I}},\ a^{\text{II}},\ a^{\text{III}},\ a^{\text{IV}}, \ldots P,\ Q,\ R,$$
$$y = b,\ b^{\text{I}},\ b^{\text{II}},\ b^{\text{III}},\ b^{\text{IV}}, \ldots S,\ T,\ V,$$

ubi secundi termini ita debent accipi, ut sit

$$a^{\mathrm{I}} = pa + qb, \quad b^{\mathrm{I}} = \alpha qa + pb;$$

deinde utraque series est recurrens scala relationis existente $2p, -1$. Erit scilicet

$$a^{\mathrm{II}} = 2pa^{\mathrm{I}} - a \quad \text{et in genere} \quad R = 2pQ - P,$$
$$b^{\mathrm{II}} = 2pb^{\mathrm{I}} - b \quad \ldots\ldots\ldots \quad V = 2pT - S;$$

ambae vero series etiam retrorsum continuari debent sicque duplo plures prodibunt solutiones, nisi sit vel $a = 0$ vel $b = 0$. Neque autem hic in censum veniunt solutiones negativae, quia, si satisfecerit $x = v$, etiam satisfacit $x = -v$. Omnes porro istae solutiones continentur in his formulis generalibus

$$x = \frac{1}{2\sqrt{\alpha}}(a\sqrt{\alpha} + b)(p + q\sqrt{\alpha})^{n} + \frac{1}{2\sqrt{\alpha}}(a\sqrt{\alpha} - b)(p - q\sqrt{\alpha})^{n},$$
$$y = \frac{1}{2}(a\sqrt{\alpha} + b)(p + q\sqrt{\alpha})^{n} - \frac{1}{2}(a\sqrt{\alpha} - b)(p - q\sqrt{\alpha})^{n}.$$

Pro variis igitur numeris, qui coefficientem α constituunt, sequentia exempla evolvamus, et quidem generalius, ut etiam coefficientis β ratio habeatur, pro casibus scilicet, quibus forte $\frac{\beta}{2\alpha}(p-1)$ fuerit numerus integer.[1])

EXEMPLUM 1

22. *Proposita formula*

$$\sqrt{(2xx + \beta x + \gamma)} = y$$

invenire infinitos valores integros ipsius x, quibus haec formula rationalis evadit, siquidem una solutio constet.

Sit solutio cognita $x = a$ et $y = b$ et ob $\alpha = 2$ habebimus $p = \sqrt{(2qq+1)}$ ideoque $q = 2$ et $p = 3$. Hinc secundi valores erunt

$$a^{\mathrm{I}} = 3a \pm 2b + \frac{\beta}{2}, \quad b^{\mathrm{I}} = 4a \pm 3b + \beta.$$

1) In editione principe exempla sequentia nonnullos errores continent, qui etiam in *Comment. arithm.* inveniuntur, hac in editione autem correcti sunt. F. R.

Cum igitur in § 19 sit

$$R = 6Q - P + \beta \quad \text{et} \quad V = 6T - S,$$

habebimus sequentes series valorum satisfacientium, et quidem integrorum, si β fuerit numerus par:

Valores ipsius x	Valores ipsius y
$a,$	$\pm\ b,$
$3a \pm 2b + \frac{\beta}{2},$	$4a \pm 3b + \beta,$
$17a \pm 12b + 4\beta,$	$24a \pm 17b + 6\beta,$
$99a \pm 70b + \frac{49}{2}\beta,$	$140a \pm 99b + 35\beta,$
$577a \pm 408b + 144\beta,$	$816a \pm 577b + 204\beta,$
$3363a \pm 2378b + \frac{1681}{2}\beta$	$4756a \pm 3363b + 1189\beta$
etc.	etc.

Tum vero, cum y eosdem retineat valores, si pro x scribatur $-x-\frac{\beta}{2}$, etiam hae solutiones locum habebunt:

Valores ipsius x	Valores ipsius y
$-a - \frac{1}{2}\beta,$	$\pm\ b,$
$-3a \mp 2b - \beta,$	$4a \pm 3b + \beta,$
$-17a \mp 12b - \frac{9}{2}\beta,$	$24a \pm 17b + 6\beta,$
$-99a \mp 70b - 25\beta,$	$140a \pm 99b + 35\beta,$
$-577a \mp 408b - \frac{289}{2}\beta,$	$816a \pm 577b + 204\beta,$
$-3363a \mp 2378b - 841\beta$	$4756a \pm 3363b + 1189\beta$
etc.	etc.

Etiamsi ergo β non fuerit numerus par, tamen in utroque ordine semissis valorum ipsius x fuerit numeri integri.

EXEMPLUM 2

23. *Proposita formula*

$$\sqrt{(3xx+\beta x+\gamma)}=y$$

invenire infinitos valores integros ipsius x, quibus haec formula rationalis evadit, siquidem unus casus constet.

Praebeat casus cognitus $x=a$ et $y=b$, tum vero ob $\alpha=3$ capiatur $p=\sqrt{(3qq+1)}$ eritque $q=1$ et $p=2$. Hinc pro secundo casu habebimus

$$a^{\mathrm{I}}=2a\pm b+\frac{\beta}{6},\quad b^{\mathrm{I}}=3a\pm 2b+\frac{1}{2}\beta,$$

ex quibus formentur binae series recurrentes secundum has scalas relationis

$$R=4Q-P+\frac{\beta}{3},\quad V=4T-S,$$

unde obtinentur:

Valores ipsius x	Valores ipsius y
$a,$	$\pm b,$
$2a\pm b+\frac{1}{6}\beta,$	$3a\pm 2b+\frac{1}{2}\beta,$
$7a\pm 4b+\beta,$	$12a\pm 7b+2\beta,$
$26a\pm 15b+\frac{25}{6}\beta,$	$45a\pm 26b+\frac{15}{2}\beta,$
$97a\pm 56b+16\beta,$	$168a\pm 97b+28\beta,$
$362a\pm 209b+\frac{361}{6}\beta,$	$627a\pm 362b+\frac{209}{2}\beta,$
$1351a\pm 780b+225\beta$	$2340a\pm 1351b+390\beta$
etc.	etc.

Praeterea vero scribendo $-x-\frac{\beta}{3}$ pro x prodibunt:

Valores ipsius x	Valores ipsius y
$-a-\frac{1}{3}\beta,$	$\pm b,$
$-2a\mp b-\frac{1}{2}\beta,$	$3a\pm 2b+\frac{1}{2}\beta,$
$-7a\mp 4b-\frac{4}{3}\beta,$	$12a\pm 7b+2\beta,$
$-26a\mp 15b-\frac{9}{2}\beta,$	$45a\pm 26b+\frac{15}{2}\beta,$
$-97a\mp 56b-\frac{49}{3}\beta,$	$168a\pm 97b+28\beta,$
$-362a\mp 209b-\frac{121}{2}\beta,$	$627a\pm 362b+\frac{209}{2}\beta,$
$-1351a\mp 780b-\frac{676}{3}\beta$	$2340a\pm 1351b+390\beta$
etc.	etc.

Prout ergo numerus β divisibilis fuerit per 2 vel 3 vel utrumque, hinc eo plures solutiones in integris eliciuntur.

EXEMPLUM 3

24. *Proposita formula*

$$\sqrt{(5xx+\beta x+\gamma)}=y$$

invenire infinitos valores integros ipsius x, quibus haec formula rationalis evadat, siquidem unus casus fuerit cognitus.

Pro casu cognito sit $x=a$ et $y=b$ et ob $\alpha=5$ quaerantur numeri p et q, ut sit $p=\sqrt{(5qq+1)}$. Fiet ergo $q=4$ et $p=9$ et hinc secunda solutio prodibit

$$a^{\text{I}}=9a\pm 4b+\frac{4}{5}\beta,\quad b^{\text{I}}=20a\pm 9b+2\beta.$$

Cum ergo sit

$$a^{\text{II}}=18a^{\text{I}}-a+\frac{8}{5}\beta \quad \text{et} \quad b^{\text{II}}=18b^{\text{I}}-b,$$

sequentes solutiones habebuntur:

Valores ipsius x	Valores ipsius y
a,	$\pm b$.
$9a \pm 4b + \frac{4}{5}\beta$,	$20a \pm 9b + 2\beta$,
$161a \pm 72b + 16\beta$,	$360a \pm 161b + 36\beta$,
$2889a \pm 1292b + \frac{1444}{5}\beta$	$6460a \pm 2889b + 646\beta$
etc.	etc.;

ubi pro quolibet valore ipsius x etiam poni potest $-x-\frac{\beta}{5}$.

SCHOLION 1

25. Cum hoc modo ex una solutione in integris cognita infinitae aliae solutiones etiam in integris eliciantur, quaestio nascitur, an hoc modo omnes plane solutiones integrae obtineantur necne. Ac in exemplis quidem primo et secundo nullum erit dubium, quin hac methodo omnes solutiones integrae obtineantur. Verum in exemplo tertio utique dantur casus, quibus multo plures solutiones in integris exhiberi possunt, quam quidem hac methodo reperiuntur. Veluti si proposita fuerit formula $\sqrt{(5xx+4)}=y$, quae pro casu cognito praebet $a=0$ et $b=2$, nostra solutio dat:

Valores ipsius x	Valores ipsius y
0,	2,
8,	18,
144,	322,
2584	5778
etc.	etc.

Verum hanc formulam diligentius scrutanti patebit non solum his casibus $\sqrt{(5xx+4)}$ fieri rationalem, sed etiam istis numeris pro x substituendis

$$x=0,\quad 1,\quad 3,\quad 8,\quad 21,\quad 55,\quad 144,\quad 377,\quad 987\quad \text{etc.},$$

unde solutionum numerus triplicatur. Cuius rei ratio est, quod ad formulam $p=\sqrt{(5qq+1)}$ resolvendam posuimus $q=4$, unde fit $p=9$; quae quidem est simplicissima solutio in numeris integris. At quoniam in scala relationis

inest $2p$, ea numeris integris constabit, etiamsi p sit fractio denominatorem habens 2. Hanc ob rem istas simpliciores solutiones nanciscemur, si ponamus $q = \frac{1}{2}$, unde fit $p = \frac{3}{2}$; sicque ob $\alpha = 5$ secundi valores erunt

$$a' = \frac{3}{2}a \pm \frac{1}{2}b + \frac{1}{20}\beta, \quad b' = \frac{5}{2}a \pm \frac{3}{2}b + \frac{1}{4}\beta$$

ac tertii cum sequentibus per hanc legem suppeditabuntur

$$a'' = 3a' - a + \frac{1}{10}\beta, \quad b'' = 3b' - b,$$

unde nanciscimur hos valores:

Valores ipsius x	Valores ipsius y
$a,$	$\pm\ b,$
$\frac{3}{2}a \pm \frac{1}{2}b + \frac{1}{20}\beta,$	$\frac{5}{2}a \pm \frac{3}{2}b + \frac{1}{4}\beta,$
$\frac{7}{2}a \pm \frac{3}{2}b + \frac{1}{4}\beta,$	$\frac{15}{2}a \pm \frac{7}{2}b + \frac{3}{4}\beta,$
$9a \pm 4b + \frac{4}{5}\beta,$	$20a \pm 9b + 2\beta,$
$\frac{47}{2}a \pm \frac{21}{2}b + \frac{9}{4}\beta,$	$\frac{105}{2}a \pm \frac{47}{2}b + \frac{21}{4}\beta,$
$\frac{123}{2}a \pm \frac{55}{2}b + \frac{121}{20}\beta,$	$\frac{275}{2}a \pm \frac{123}{2}b + \frac{55}{4}\beta,$
$161a \pm 72b + 16\beta$	$360a \pm 161b + 36\beta$
etc.	etc.

Atque hinc illae triplo plures solutiones oriuntur, quoties fuerit $a \pm b$ numerus par ac β vel $= 0$ vel per 20 divisibile.

SCHOLION 2

26. Quandoque ergo plures solutiones in numeris integris reperiuntur, si pro p et q fractiones cum denominatore 2 assumuntur; quod quando in genere eveniat, operae pretium erit investigasse. Plerumque autem hi casus locum non habent, nisi sit vel $\beta = 0$ vel formula ad talem formam reduci possit. Sit ergo proposita formula $\sqrt{(\alpha xx + \gamma)} = y$, cui satisfaciat casus

$x = a$ et $y = b$; tum statuatur $p = \frac{m}{2}$ et $q = \frac{n}{2}$ seu quaerantur numeri m et n, ut sit $mm = ann + 4$ et $m = \sqrt{(ann + 4)}$. Tum vero solutio prima statim dat secundam

$$a^{\text{I}} = \frac{ma + nb}{2} \quad \text{et} \quad b^{\text{I}} = \frac{ana + mb}{2},$$

ubi quidem numeri m et n tam negative quam affirmative accipi possunt. Denique his binis primis inventis sequentes per hanc regulam reperientur

$$a^{\text{II}} = ma^{\text{I}} - a \quad \text{et} \quad b^{\text{II}} = mb^{\text{I}} - b.$$

In genere autem quilibet numerus pro x satisfaciens continetur hac formula

$$x = \frac{1}{2\sqrt{a}}(a\sqrt{a} + b)\left(\frac{m + n\sqrt{a}}{2}\right)^{\mu} + \frac{1}{2\sqrt{a}}(a\sqrt{a} - b)\left(\frac{m - n\sqrt{a}}{2}\right)^{\mu},$$

ex qua fit

$$y = \frac{1}{2}(a\sqrt{a} + b)\left(\frac{m + n\sqrt{a}}{2}\right)^{\mu} - \frac{1}{2}(a\sqrt{a} - b)\left(\frac{m - n\sqrt{a}}{2}\right)^{\mu}.$$

Quoties igitur $ma + nb$ prodierit numerus par neque tamen m et n sint pares, toties triplo plures solutiones in integris prodeunt quam methodo praecedente. Hae vero solutiones ita se habebunt:

$$a = a, \qquad b = b,$$

$$a^{\text{I}} = \frac{ma + nb}{2}, \qquad b^{\text{I}} = \frac{mb + ana}{2},$$

$$a^{\text{II}} = \frac{(mm - 2)a + mnb}{2}, \qquad b^{\text{II}} = \frac{(mm - 2)b + amna}{2},$$

$$a^{\text{III}} = \frac{(m^3 - 3m)a + (mm - 1)nb}{2}, \qquad b^{\text{III}} = \frac{(m^3 - 3m)b + a(mm - 1)na}{2},$$

$$a^{\text{IV}} = \frac{(m^4 - 4mm + 2)a + (m^3 - 2m)nb}{2}, \qquad b^{\text{IV}} = \frac{(m^4 - 4mm + 2)b + a(m^3 - 2m)na}{2},$$

$$a^{\text{V}} = \frac{(m^5 - 5m^3 + 5m)a + (m^4 - 3mm + 1)nb}{2}, \qquad b^{\text{V}} = \frac{(m^5 - 5m^3 + 5m)b + a(m^4 - 3mm + 1)na}{2}$$

etc.

OBSERVATIO 1

27. Haec altera methodus tum demum plures solutiones in numeris integris suppeditat quam prior, cum m et n fuerint numeri impares simulque

a et b ambo vel pares vel impares. Si enim m et n sint numeri pares, p et q erunt integri et formula $m = \sqrt{(ann + 4)}$ easdem solutiones praebebit ac formula $p = \sqrt{(aqq + 1)}$. Deinde si $ma + nb$ non fuerit numerus par, valores a', a'' non evadent integri neque propterea plures solutiones reperiuntur quam priore methodo, dum adhibetur formula $p = \sqrt{(aqq + 1)}$. Distingui ergo oportet eos casus, quibus formulae $m = \sqrt{(ann + 4)}$ numeris imparibus pro m et n accipiendis satisfieri potest, id quod statim patet fieri non posse, si a fuerit numerus formae $4z - 1$ vel etiam huius $8z + 1$. Quare pro a alii numeri impares non relinquuntur, nisi qui sint formae $8z + 5$[1]). Pro his ergo casibus minimos valores formulae $m = \sqrt{(ann + 4)}$ satisfacientes sequens tabella exhibet:

Si fuerit	capiatur	eritque
$a = 5$,	$n = 1$	$m = 3$,
$a = 13$,	$n = 3$	$m = 11$,
$a = 21$,	$n = 1$	$m = 5$,
$a = 29$,	$n = 5$	$m = 27$,
$a = 37$,	$n =$ —	$m =$ —
$a = 45$,	$n = 1$	$m = 7$,
$a = 53$,	$n = 7$	$m = 51$,
$a = 61$,	$n = 195$	$m = 1523$,
$a = 69$,	$n = 75$	$m = 623$,
$a = 77$,	$n = 1$	$m = 9$,
$a = 85$,	$n = 9$	$m = 83$,
$a = 93$,	$n = 87$[2])	$m = 839$.

Quaeritur hic ratio, cur casus $a = 37$ non recipiat valores impares pro m et n. Hic igitur patet, si sit $a = 37$, non dari numeros impares pro m et n; pro reliquis autem casibus resolutio succedit.

Ita si proponatur haec formula

$$\sqrt{(53xx + 28)} = y,$$

habetur statim $a = 1$ et $b = 9$. Deinde ob $n = 7$ et $m = 51$ erit

$$a' = \frac{51 + 63}{2} = 57 \quad \text{et} \quad b' = \frac{371 + 459}{2} = 415,$$

1) Editio princeps (atque etiam *Comment. arithm.*): $4z + 5$. Correxit F. R.

2) Editio princeps (atque etiam *Comment. arithm.*): $n = 57$. Correxit F. R.

seu etiam

$$a' = -6 \quad \text{et} \quad b' = -44;$$

et series recurrentes pro x et y, quarum scala relationis est 51, — 1, erunt:

$$x = \text{etc.} \quad -307, \quad -6, \quad 1, \quad 57, \quad 2906 \quad \text{etc.},$$
$$y = \text{etc.} \quad 2235, \quad 44, \quad 9, \quad 415, \quad 21156 \quad \text{etc.}$$

OBSERVATIO 2

28. Sufficit autem casus evolvisse, quibus in formula generali $\alpha xx + \beta x + \gamma$ secundus terminus deest, quoniam haec ad talem formam salva numerorum integritate revocari potest. Vulgaris quidem modus, quo ex aequationibus secundus terminus tolli solet ponendo $x = y - \frac{\beta}{2\alpha}$, hic locum habere nequit, nisi β sit numerus per 2α divisibilis. Verum si $\alpha xx + \beta x + \gamma$ debeat esse quadratum, ponatur

$$\alpha xx + \beta x + \gamma = yy$$

ac multiplicando per 4α prodibit

$$4\alpha\alpha xx + 4\alpha\beta x + 4\alpha\gamma = 4\alpha yy$$

ideoque

$$4\alpha yy + \beta\beta - 4\alpha\gamma = (2\alpha x + \beta)^2.$$

Quaerantur ergo casus, quibus formula $4\alpha yy + \beta\beta - 4\alpha\gamma$ fit quadratum, indeque habebuntur valores pro x substituendi, qui formulam $\alpha xx + \beta x + \gamma$ reddant quadratam; scilicet si fuerit

$$\sqrt{(4\alpha yy + \beta\beta - 4\alpha\gamma)} = z,$$

erit $2\alpha x + \beta = z$ hincque

$$x = \frac{z - \beta}{2\alpha}.$$

Quodsi β fuerit numerus par, puta 2δ, posito $\alpha xx + 2\delta x + \gamma = yy$ erit

$$(\alpha x + \delta)^2 = \alpha yy + \delta\delta - \alpha\gamma$$

sicque formula $\alpha yy + \delta\delta - \alpha\gamma$ ad quadratum est revocanda; ac si invenimus

$$\sqrt{(\alpha yy + \delta\delta - \alpha\gamma)} = z,$$

erit $\alpha x + \delta = z$ et

$$x = \frac{z - \delta}{\alpha},$$

unde plerumque pro x numeri integri reperiuntur; etsi enim forte $\frac{z-\delta}{\alpha}$ non fuerit integer, tamen ex uno valore z cognito, si modo supra tradito alii eliciantur in infinitum, alterni saltem erunt numeri integri. Ex quo perspicuum est resolutionem formularum quadraticarum radicalium $\sqrt{(\alpha xx+\beta x+\gamma)}$ nulla limitatione affici, etiamsi terminus βx plane omittatur, sicque totum negotium huc redit, ut formulae huiusmodi $\sqrt{(\alpha xx+\gamma)}$ rationales et quidem in numeris integris reddantur.

OBSERVATIO 3

29. Iam annotavi formulam $\alpha xx+\gamma$ in numeris integris saltem pluribus ac infinitis modis quadratum effici non posse, nisi α sit numerus positivus non quadratus. Existente autem α tali numero problema non ita resolvi potest, ut pro quocunque numero pro γ assumto solutio succedat; possent enim utique eiusmodi numeri pro γ dari, ut problema nullam plane solutionem admitteret, atque hanc ob rem postulavi unam saltem solutionem cognitam esse debere, quo ipso casus insolubiles exclusi.

Verum dato α characteres exhiberi possunt, ex quibus dignosci liceat, utrum numerus γ sit eiusmodi, qui solutionem admittat necne. Ac primo quidem perspicuum est nullam solutionem locum habere posse, nisi γ sit numerus in tali formula $bb-\alpha aa$ contentus. Dato ergo numero α formetur series omnium numerorum tam positivorum quam negativorum, qui quidem in formula $bb-\alpha aa$ sint contenti; ac nisi γ in hac serie reperiatur, certo pronunciare licet formulam $\sqrt{(\alpha xx+\gamma)}$ nullo modo rationalem reddi posse; vicissim autem quoties γ in hac serie comprehenditur, quia tum est $\gamma=bb-\alpha aa$, formula $\alpha xx+\gamma$ fit quadratum ponendo $x=a$ eritque $\sqrt{(\alpha xx+\gamma)}=b$.

Haec igitur series, cuius quasi terminus generalis est $bb-\alpha aa$, primo continebit sumto $a=0$ omnes numeros quadratos

$$1, \quad 4, \quad 9, \quad 16, \quad 25 \text{ etc.},$$

tum vero omnes quadratos per $-\alpha$ multiplicatos, nempe

$$-\alpha, \quad -4\alpha, \quad -9\alpha, \quad -16\alpha \text{ etc.}$$

Praeterea si p et q fuerint numeri in hac serie contenti, in ea quoque reperietur eorum productum pq; nam cum sit

$$p = bb - aaa \quad \text{et} \quad q = dd - acc,$$

erit

$$pq = (bd \pm aac)^2 - a(bc \pm ad)^2$$

et ob ambiguitatem signi hoc productum duplici modo est numerus formae $bb - aaa$ ideoque statim habentur duae solutiones

$$x = bc + ad \quad \text{et} \quad x = bc - ad.$$

OBSERVATIO 4

30. Hinc ergo consecuti sumus hoc Theorema eximium[1], quod fundamentum superiorum solutionum in se complectitur:

Si fuerit

$$axx + p = yy$$

casu $x = a$ et $y = b$, tum vero etiam

$$axx + q = yy$$

casu $x = c$ et $y = d$, haec formula

$$axx + pq = yy$$

adimplebitur capiendo

$$x = bc \pm ad \quad \text{et} \quad y = bd \pm aac.$$

Si enim sit $q = 1$ et $dd = acc + 1$, praeterea vero formulae $axx + p = yy$ satisfiat casu $x = a$ et $y = b$, qui est casus supra pro cognito assumtus, tum eidem formulae satisfacient valores

$$x = bc \pm ad \quad \text{et} \quad y = bd \pm aac,$$

unde eadem omnino solutio conficitur, quam supra exhibuimus atque ex

1) Vide epistolam a CHR. GOLDBACH d. 28. Iunii 1753 ad EULERUM scriptam, *Correspondance math. et phys. publiée par P. H. FUSS*, St.-Pétersbourg 1843, t. I, p. 610; *LEONHARDI EULERI Opera omnia*, series III.

EULERUS scire nequivit hoc theorema iam Celeb. BHÂSKARA (n. a. 1114) Mathematico indico cognitum fuisse. Vide *Algebra, with Arithmetic and Mensuration from the Sanscrit of BRAHMEGUPTA and BHÀSCARA.* Translated by H. TH. COLEBROOKE, London 1817, *Algebra* (*Vijaganita*), chap. III, p. 170–184, imprimis p. 171. Vide etiam H. HANKEL, *Zur Geschichte der Mathematik in Altertum und Mittelalter*, Leipzig 1874, p. 200, atque M. CANTOR, *Vorlesungen über Geschichte der Mathematik*, Bd. 1, 3. Aufl., Leipzig 1907, p. 633. F. R.

longe diversis principiis elicuimus; quocirca haec postrema investigationis ratio ob concinnitatem et perspicuitatem eo magis est notatu digna. Hic vero accedit, quod haec ratio multo latius pateat quam praecedens, quippe quae ad casum $q = 1$ fuerat adstricta. Demonstratio autem istius Theorematis elegantissimi ita brevissime se habebit.

Cum sit

$$aaa + p = bb,$$

erit

$$p = bb - aaa$$

et ob

$$acc + q = dd$$

erit

$$q = dd - acc;$$

hinc erit $pq = (bb - aaa)(dd - acc)$, quae expressio reducitur ad hanc

$$pq = (bd \pm aac)^2 - a(bc \pm ad)^2.$$

Quodsi ergo fuerit

$$x = bc \pm ad \quad \text{et} \quad y = bd \pm aac,$$

erit $pq = yy - axx$ ideoque

$$axx + pq = yy.$$

Q. E. D.

OBSERVATIO 5

31. Cum igitur pro quolibet numero a formulae $axx + \gamma = yy$ numerus γ debeat esse formae $bb - aaa$, numeri in hac forma contenti diligentius examinari merentur; et quoniam, si inter eos occurrunt numeri p et q, simul quoque eorum productum pq occurrit, praeter numeros quadratos 1, 4, 9, 16, 25 etc. eorumque multipla negativa $-a$, $-4a$, $-9a$, $-16a$, $-25a$ etc. imprimis numeri primi in hac forma contenti sunt spectandi, quippe ex quibus deinceps per multiplicationem compositi nascuntur[1]).

I. Sit $a = 2$ et numeri primi formae $bb - 2aa$ sunt

positivi $+1$, $+2$, $+7$, $+17$, $+23$, $+31$, $+41$, $+47$, $+71$, $+73$, $+79$, $+89$, $+97$ etc.,

1) Ad investigationes sequentes vide Commentationem 164 huius voluminis. F. R.

negativi -1, -2, -7, -17, -23, -31, -41, -47, -71,
-73, -79, -89, -97 etc.,

qui praeter $+2$ et -2 omnes in forma $\pm(8n \pm 1)$ continentur.

II. Sit $a = 3$ et numeri primi formae $bb - 3aa$ sunt

positivi $+1$, $+13$, $+37$, $+61$, $+73$, $+97$, $+109$ etc.,
negativi -2, -3, -11, -23, -47, -59, -71, -83, -107 etc.,

qui praeter -2 et -3 omnes continentur in forma $12n \pm 1$, siquidem pro n tam numeri positivi quam negativi capiantur.

III. Sit $a = 5$ et numeri primi formae $bb - 5aa$ sunt

positivi $+1$, $+5$, $+11$, $+19$, $+29$, $+31$, $+41$, $+59$,
$+61$, $+71$, $+79$, $+89$, $+101$ etc.,

negativi -1, -5, -11, -19, -29, -31, -41, -59,
-61, -71, -79, -89, -101 etc.,

qui praeter $+5$ et -5 omnes in forma $10n \pm 1$ continentur.

IV. Sit $a = 6$ et numeri primi formae $bb - 6aa$ sunt

positivi $+1$, $+3$, $+19$, $+43$, $+67$, $+73$, $+97$ etc.,
negativi -2, -23, -29, -47, -53, -71, -101 etc.,

qui praeter -2 et $+3$ omnes in alterutra harum formarum $24n + 1$ et $24n - 5$ continentur sumendo pro n numeros tam negativos quam positivos.

V. Sit $a = 7$ et numeri primi formae $bb - 7aa$ sunt

positivi $+1$, $+2$, $+29$, $+37$, $+53$, $+109$ etc.,
negativi -7, -3, -19, -31, -47, -59, -83 etc.,

qui praeter $+2$ et -7 omnes in una harum formarum continentur $28n + 1$, $28n + 9$, $28n + 25$.

OBSERVATIO 6

32. Hinc colligimus omnes numeros primos in formula $bb - \alpha aa$ contentos simul in quibusdam huiusmodi formulis $4\alpha n + A$ contineri, dum pro A certi quidam numeri substituuntur. Quod idem etiam hoc modo ostendi potest. Ponatur

$$b = 2\alpha p + r \quad \text{et} \quad a = 2q + s$$

ac formula $bb - \alpha aa$ transit in hanc

$$4\alpha\alpha pp + 4\alpha pr + rr - 4\alpha qq - 4\alpha qs - \alpha ss;$$

statuatur $\alpha pp + pr - qq - qs = n$ et habebimus

$$bb - \alpha aa = 4\alpha n + rr - \alpha ss.$$

Omnes ergo numeri primi formae $bb - \alpha aa$ quoque in hac forma $4\alpha n + rr - \alpha ss$ continentur; atque ut hi numeri sint primi, r et s ita accipi oportet, ut numerus $rr - \alpha ss$ sit vel ipse primus vel saltem ad 4α primus. Primo ergo sumto $s = 0$ pro r successive accipi possunt numeri impares ad α primi, ac si rr fuerit maius quam 4α, inde 4α toties subtrahatur, quoties fieri potest, ut residuum sit minus quam 4α, et quot hoc modo diversi numeri resultant, ii in formula $4\alpha n + A$ loco A collocentur. Deinde etiam simili modo colligantur numeri ex formulis $rr - \alpha$, qui, quatenus sunt diversi, ad illos insuper adiiciantur. Non autem opus est pro s alios numeros praeter unitatem assumere; si enim s esset numerus par, numerus $-\alpha ss$ iam in forma $4\alpha n$ contineretur, et si s esset impar, numerus $-\alpha ss$ haberet formam $-4\alpha N - \alpha$, cuius pars $-4\alpha N$ iam in $4\alpha n$ continetur, sicque sufficit pro formulis $4\alpha n + A$ quovis casu has $4\alpha n + rr$ et $4\alpha n + rr - \alpha$ evolvere eaeque iam omnes numeros primos, qui quidem in formula $bb - \alpha aa$ comprehenduntur, in se complectentur. Num autem vicissim omnes numeri primi in his formulis $4\alpha n + rr$ et $4\alpha n + rr - \alpha$ contenti simul sint numeri formae $bb - \alpha aa$, quaestio est altioris indaginis, quae tamen affirmanda videtur[1]).

1) Hoc vero locum non habere primum annotavit I. L. LAGRANGE demonstrando numerum primum $n = 101$, qui pro casu $\alpha = 79$ in forma $4\alpha n + r^2 - \alpha$ continetur ($n = -4$, $r = 38$), nullo modo per formam $b^2 - 79a^2$ repraesentari posse. Vide I. L. LAGRANGE, *Additions à l'analyse indéterminée* (*Élémens d'algèbre par M. L. Euler, traduits de l'Allemand, avec des notes et des additions*, Lyon 1774, t. II, p. 620—623); *LEONHARDI EULERI Opera omnia*, series I, vol. 1, p. 628—630. F. R.

OBSERVATIO 7

33. Quo haec exemplo illustremus, sit $a = 13$ et ex $4an + rr$ et $4an + rr - a$ orientur hae formulae pro numeris primis

ex $4an + rr$	ex $4an + rr - a$
$52n + 1$,	$52n - 9$,
$52n + 9$,	$52n + 3$,
$52n + 25$,	$52n + 23$,
$52n + 49 = 52n - 3$,	$52n + 51 = 52n - 1$,
$52n + 81 = 52n - 23$,	$52n + 87 = 52n - 17$,
$52n + 121 = 52n + 17$,	$52n + 131 = 52n - 25$,

quae formulae reducuntur ad has

$$52n \pm 1,\quad 52n \pm 3,\quad 52n \pm 9,\quad 52n \pm 17,\quad 52n \pm 23,\quad 52n \pm 25;$$

ac numeri primi in his contenti sunt

$$\pm 1,\ \pm 3,\ \pm 17,\ \pm 23,\ \pm 29,\ \pm 43,\ \pm 53,\ \pm 61,\ \pm 79,\ \pm 101,\ \pm 103,$$

quibus addi debet ± 13, tum vero omnes numeri quadrati; atque si insuper adiiciantur producta ex binis pluribusque horum numerorum, obtinebuntur hoc quidem casu omnes numeri, qui pro y substituti producunt formulam $13xx + y = yy$ in numeris integris resolubilem; seu quicunque illorum numerorum pro y accipiatur, unus primo, deinde infiniti numeri integri pro x inveniri possunt, quibus formula $13xx + y$ quadratum reddatur. Omnes enim isti numeri simul in forma $bb - 13aa$ continentur; qui enim hoc difficiliores reducta videntur, sunt:

$$-1 = 18^2 - 13 \cdot 5^2,\qquad +13 = 65^2 - 13 \cdot 18^2,\qquad -3 = 7^2 - 13 \cdot 2^2,$$
$$+17 = 15^2 - 13 \cdot 4^2,\qquad -17 = 10^2 - 13 \cdot 3^2,\qquad -23 = 43^2 - 13 \cdot 12^2,$$
$$+29 = 9^2 - 13 \cdot 2^2,\qquad -29 = 32^2 - 13 \cdot 9^2,\qquad +43 = 76^2 - 13 \cdot 21^2,$$
$$-43 = 3^2 - 13 \cdot 2^2,\qquad +53 = 51^2 - 13 \cdot 14^2,\qquad -53 = 8^2 - 13 \cdot 3^2,$$
$$+61 = 23^2 - 13 \cdot 6^2,\qquad -61 = 24^2 - 13 \cdot 7^2,\qquad +79 = 14^2 - 13 \cdot 3^2,$$
$$-79 = 57^2 - 13 \cdot 16^2 \text{ [1]) etc.}$$

1) Editio princeps (atque etiam *Comment. arithm.*): $-79 = 16^2 - 13 \cdot 5^2$. Correxit F. R.

Cum ergo sit $1 = 18^2 - 13 \cdot 5^2$, si fuerit $+\gamma = bb - 13aa$, erit

$$\gamma = (18b \pm 65a)^2 - 13(18a \pm 5b)^2,$$

unde casus difficiliores resolvuntur.

Proposita ergo resolvenda hac aequatione

$$13xx + 43 \cdot 79 = yy,$$

cum sit $\gamma = 43 \cdot 79 = -43 \cdot -79$, habebitur per compositionem

$$\text{I.} \quad \gamma = (14 \cdot 76 \pm 13 \cdot 63)^2 - 13(14 \cdot 21 \pm 3 \cdot 76)^2,$$

ergo

$$x = 294 \pm 228 \quad \text{et} \quad y = 1064 \pm 819,$$

$$\text{II.} \quad \gamma = (3 \cdot 57 \pm 13 \cdot 32)^2 - 13(2 \cdot 57 \pm 3 \cdot 16)^2,\text{[1]}$$

ergo

$$x = 114 \pm 48 \quad \text{et} \quad y = 416 \pm 171,\text{[2]}$$

unde statim tres solutiones obtinentur.[3]

OBSERVATIO 8

34. Verum non semper ex his numeris primis, quos modo investigare docuimus, cum quadratis omnes plane numeri, qui pro γ assumi possunt, reperiuntur, cuius rei exemplum est casus $a = 10$, pro quo valores ipsius γ in hac forma $bb - 10aa$ continentur; iique sunt tam negative quam positive sumti

1, 4, 6, 9, 10, 15, 16, 24, 25, 26, 31, 36, 39, 40, 41, 49, 54, 60, 64, 65, 71, 74, 79, 81, 86, 89, 90, 96, 100, 104, 106, 111, 121, 124, 129, 134, 135, 144, 150, 151, 156, 159, 160, 164, 166, 169, 185, 186, 191, 196, 199, 201 etc.,

1) Editio princeps: $\gamma = (3 \cdot 16 \pm 13 \cdot 10)^2 - 13(2 \cdot 16 \pm 3 \cdot 5)^2$. Correxit F. R.

2) Editio princeps: $x = 32 \pm 15$ *et* $y = 130 \pm 48$. Correxit F. R.

3) Editio princeps: *unde statim 4 solutiones obtinentur*. Revera autem tres tantum solutiones reperiuntur, scilicet

$$x = 522, \quad y = 1883,$$
$$x = 66, \quad y = 245,$$
$$x = 162, \quad y = 587.$$

Quarta enim solutio cum secunda convenit. F. R.

inter quos numeros occurrunt primo omnes quadrati

$$1,\ 4,\ 9,\ 16,\ 25,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 144,\ 169,\ 196\ \textit{etc.},$$

deinde numeri primi

$$31,\ 41,\ 71,\ 79,\ 89,\ 151,\ 191,\ 199\ \textit{etc.},$$

qui in his formulis continentur $40n \pm 1$ et $40n \pm 9$, insuperque accedunt producta ex binis pluribusve horum numerorum. Tertio vero praeter hos adsunt numeri ex binis numeris primis compositi, qui sunt

$$2\cdot 3,\ 2\cdot 5,\ 2\cdot 13,\ 2\cdot 37,\ 2\cdot 43,\ 2\cdot 53,\ 2\cdot 67,\ 2\cdot 83\ \textit{etc.},$$
$$3\cdot 5,\ 3\cdot 13,\ 3\cdot 37,\ 3\cdot 43,\ 3\cdot 53,\ 3\cdot 67\ \textit{etc.},$$
$$5\cdot 13,\ 5\cdot 37\ \textit{etc.}$$

At hi numeri primi, quorum semper bini sunt in se multiplicandi, sunt primo 2 et 5, reliqui vero in his formulis continentur $40n \pm 3$ et $40n \pm 13$. Denique etiam secundum regulam generalem adiici debent producta ex binis pluribusve numeris, qui per se satisfaciunt.

Ita resolvi poterit haec aequatio

$$10zz + 13\cdot 53\cdot 151 = yy,$$

nam est $13\cdot 53 = bb - 10aa$ existente $b = 27$ et $a = 2$ et $151 = dd - 10cc$ existente $d = 31$ et $c = 9$ hincque

$$13\cdot 53\cdot 151 = (bd \pm 10ac)^2 - 10(ad \pm bc)^2$$

et

$$z = ad \pm bc \quad \text{et} \quad y = bd \pm 10ac.$$

Deinde cum etiam sit $-13\cdot 53 = BB - 10AA$ et $-151 = DD - 10CC$, hinc duae aliae solutiones reperiuntur. Cum autem sit $-1 = 3^2 - 10\cdot 1^2$, si fuerit $\gamma = bb - 10aa$, erit $-\gamma = (3b \pm 10a)^2 - 10(3a \pm b)^2$. Solutiones autem hinc oriundae sunt

$$z = 181, \qquad y = 657,$$
$$z = 305, \qquad y = 1017,$$
$$z = 307, \qquad y = 1023;$$

duae enim inter se conveniunt, ita ut hinc tres tantum reperiantur[1]).

1) Revera non tres, sed sex solutiones hac computatione reperiuntur. Ob ambiguitatem enim istorum valorum A, B, C, D oriuntur etiam sequentes solutiones:

OBSERVATIO 9

35. Hoc ergo casu $a = 10$ pro γ triplicis generis numeros primitivos invenimus, primo scilicet numeros quadratos omnes, deinde certos numeros primos in formulis $40n + 1$ et $40n \pm 9$ contentos, tertio autem producta ex binis certis numeris primis, qui sunt 2, 5 et reliqui ex his formulis $40n \pm 3$ et $40n + 13$ petendi, atque ex hoc demum triplici ordine omnes numeri pro γ idonei formantur, ut huic aequationi $10xx + \gamma = yy$ satisfieri possit. Ipsi autem numeri primi in formulis $40n \pm 3$ et $40n \pm 13$ contenti non conveniunt, quia non sunt formae $bb - 10aa$, sed tamen hi numeri omnes sunt formae $2bb - 5aa$, uti etiam duo iis iungendi 2 et 5. Manifestum autem est, si habeantur duo numeri huiusmodi $2bb - 5aa$ et $2dd - 5cc$, eorum productum fore $= (2bd + 5ac)^2 - 10(bc \pm ad)^2$ ideoque pro γ adhiberi posse. Huiusmodi igitur producta binorum numerorum primorum, qui ipsi non satisfaciunt, occurrere nequeunt, si a fuerit numerus primus, sed tantum, uti hic usu venit, si a fuerit numerus compositus; quod tamen etiam non semper locum habet, uti vidimus casu $a = 6 = 2 \cdot 3$, quo numeri formae $3bb - 2aa$ conveniunt cum numeris formae $bb - 6aa$. Quodsi ergo in genere fuerit $a = pq$ et aequatio $pqxx + \gamma = yy$ resolvi debeat, numerus γ vel esse debet numerus quadratus vel primus formae $bb - pqaa$ vel productum ex duobus numeris primis formae $pbb - qaa$, propterea quod huiusmodi productum est

$$(pbb - qaa)(pdd - qcc) = (pbd \pm qac)^2 - pq(bc \pm ad)^2.$$

Nisi ergo tales numeri primi iam ipsi $pbb - qaa$ in forma $bb - pqaa$ contineantur, tertius ille ordo numerorum ex binis numeris primis conflatorum accedit. Quemadmodum deinde numeri primi solitarii continentur in formulis

$$4pqn + rr \quad \text{et} \quad 4pqn + rr - pq,$$

ita numeri primi alteri combinandi ex formula hac

$$4pqn + prr - qss$$

derivari debent.

$$z = 503, \quad y = 1623,$$
$$z = 7381, \quad y = 23343,$$
$$z = 11897, \quad y = 37623;$$

utraque autem solutio $z = 181$, $y = 657$ et $z = 305$, $y = 1017$ adeo ter invenitur. F. R.